NEW YORK STATE | Office of Information Technology Services

KATHY HOCHUL
Governor

DRU RAI
NYS Chief Information Officer

November 5, 2024

Sent via email to: kstokley@thundercattech.com

Kent Stokley
Director
Thundercat Technology
11190 Sunrise Valley Drive, Suite 200
Reston, VA 20191

RE: REQUEST FOR QUOTE # ITS-2024-315DB-Google Cloud SA

Dear Kent Stokley: :

Thank you for submitting a quote in response to the above referenced RFQ conducted by the NYS Office of Information Technology Services (ITS). I am writing to advise you Thundercat Technology has submitted the lowest responsive quote and will receive a tentative award for this procurement. Congratulations. A purchase order will be issued in the near future.

Thank you again for your interest in our business.

Sincerely,

Elaine K Blanchet

Elaine Blanchet
Assistant Director, VSMO

Office of Information Technology Services
Vendor Sourcing and Management
Swan Street Building Core 4 - Room 2404
Albany, New York 12223

Cover Page – Request for Quote – Cloud Solution

TO BE COMPLETED BY AUTHORIZED USER

RFQ Title **Google Cloud SA** **RFQ Number** ITS-2024-526DB

Authorized User Information:
Office of Information Technology Services
Empire State Plaza
Swan Street Building, Core 4
2nd Floor, Room 2404
Albany, NY 12223

Authorized User Delivery Information:
Joseph Marshall
NYS Office of Information Technology Services
Swan Street Bldg, Core 4, Floor 3
Empire State Plaza
Albany, NY 12227

Special Delivery Instructions:

DESIGNATED CONTACTS

Name(s)	E-Mail(s)
Dominic Brefo – Contract Manager	Its.sm.ITS_BIDS@its.ny.gov

Authorized User shall indicate if Procurement Lobbying Law/Restricted Period is in effect: ☒ **Yes** ☐ **No**
Where Procurement Lobbying Law is deemed applicable by the Authorized User, by signing, Contractor affirms that it understands and agrees to comply with the Authorized User's policies and procedures relative to permissible contacts. Information may be accessed at: Procurement Lobbying:
http://www.ogs.ny.gov/aboutOgs/regulations/defaultAdvisoryCouncil.html)

RFQ LOTS

This RFQ is for Products from the following checked Lots as defined in Award # 22802 – Information Technology Umbrella Contract – Manufacturer Based (Statewide):

☐ Lot 1 – Software ☐ Lot 2 – Hardware ☒ Lot 3 - Cloud ☐ Lot 4 – Implementation

The Authorized User named above is seeking competitive quotes from the Contractor (Manufacturer) and their Resellers (where applicable) of Information Technology Umbrella Contract – Manufacturer Based Contract(s) for the above-referenced Products. If the RFQ includes Lot 4 – Implementation, Contractor must prior to submitting a response to the RFQ either hold an award for Lot 4- Implementation or be able to provide the services under the other Lots included in the RFQ.

LOT 3 – CLOUD DATA RISK LEVEL: ☐ Low ☒ Medium ☐ High

DATA CATEGORIZATION ELEMENTS: Data is all public information.

QUESTIONS AND OTHER EVENTS

Event	Date	Time
RFQ Release Date	11/1/2024	N/A
Questions Due	11/4/2024	3:00 PM EST
Vendor Response Due Date	11/5/2024	3:00 PM EST

IS THE RFQ BIDDER POOL LIMITED TO M/WBE, SB, AND SDVOB VENDORS: ☐ Yes ☒ No

BASIS FOR AWARD
☒ Lowest Price Meeting Specified Technical Requirements
☐ Lowest Price Meeting Specified Technical Requirements **and** Mandatory Pass/Fail Requirements
☐ Best Value with Technical and Financial Score

E-RATE ELIGIBLE ☐ Yes (E-Rate Discounts are Required) ☒ No

SERVICE MODEL FOR LOT 3 – CLOUD SOLUTION *(check all that apply)*
☒ Software as a Service (SaaS)
☒ Platform as a Service (PaaS)
☒ Infrastructure as a Service(IaaS)
☐ Anything as a Service (XaaS)

DEPLOYMENT MODEL FOR LOT 3 – CLOUD SOLUTION (*Check all that apply*)	☐ Private Cloud ☐ Community Cloud ☒ Public Cloud ☐ Hybrid Cloud ☐ Other
APPLICABLE STATUTORY / POLICY REQUIRMENT	☐ None ☒ CJIS ☐ FERPA ☒ FISMA ☒ GLB ☐ HIPAA ☐ HITECH ☐ Tax ☐ PPI ☐ PCI DSS ☐ SOX ☐ ECPA ☐ Other
CAIQ REQUIRMENT	☐ Yes ☒ No
ATTACHMENTS	Attachment 1 - Request for Quote – Financial Response – Cloud Solution Attachment 2 – Non-Collusive Bidding Certification Exhibit 1 – Google Master Terms and G Suite Service Schedule

The Authorized User will not be held liable for any cost incurred by the Contractor for work performed in the preparation of a response to this RFQ or for any work performed prior to the formal execution of an Authorized User Agreement. Responses to the RFQ must be received by the deadline specified above. Contractors assume all risks for timely, properly submitted deliveries. A Contractor is strongly encouraged to arrange for delivery of RFQ responses prior to the date of the RFQ opening. LATE RFQ responses may be rejected. The received time of a RFQ response will be determined by the Authorized User.

All purchases resulting from this RFQ shall be in accordance with terms and conditions of the OGS Information Technology Umbrella Contract – Manufacturer Based Contract and any additional terms and conditions set forth in this RFQ and its Attachments.

A. SCOPE / MANDATORY REQUIREMENTS

This RFQ is being distributed to the Contractor and Resellers (where applicable) to acquire the following:

1. SCOPE

This RFQ is seeking to acquire Google cloud data acquisition, compute, cybersecurity, and support products off Office of General Services centralized Google contract PM67982. These products will be used to provide centralized IT consolidation of agency contracts, satisfy existing agency demand and result in significant savings to the state thru centralization.

The term of this agreement is two years with the option to renew based upon mutual consent. Annual purchase orders will be issued. Payment of invoices will be made for actual usage on a monthly basis.

For the duration of an Authorized User Agreement, the Cloud Solution shall conform to the Cloud Solution Manufacturer's specifications, Documentation, performance standards (including applicable license terms, warranties, guarantees, Service Level Agreements, service commitments, and credits).

2. CLOUD SERVICE MODEL

Software as a Service (SaaS)
Infrastructure as a Service (IaaS)
Platform as a Service (PaaS)

3. CLOUD DEPLOYMENT MODEL

Public Cloud (Google Cloud Platform).

4. DATA CATEGORIZATION

Risk Level: Medium. All data is public information.

5. DATA OWNERSHIP

The Authorized User shall own all right, title and interest in Data.

6. DATA LOCATION

All Data shall remain in CONUS.

7. ENCRYPTION

Contractor shall use appropriate means to preserve and protect State Data. This includes, but is not limited to, use of stable storage Media, regular data backups and archiving, password protection of volumes, and data encryption. Encryption at rest as well as Encryption in flight within the Google Cloud infrastructure. Availability to leverage CMEK (Customer Managed Encryption Keys). All Data transmitted between ITS and the Contractor must comply with NYS ITS Standard NYS-S14-007 Encryption Standard (http://its.ny.gov/document/encryption-standard).

8. SECURITY

The Contractor and its personnel shall adhere to all required compliance domains, State security policies, procedures, and directives currently existing or implemented during the term of the Contract. These compliance domains and security policies include, but are not limited to, the following New York State Information Security Policies and Standards, National Institute of Standards and Technology (NIST) Policies (or their successor policies), and statutes:

P03-002 - Information Security Policy
P08-001 - Enterprise Plan to Procure Policy
P08-005 - Accessibility of Web-Based Information and Application
S13-002 - Information Classification Standard
S13-003 - Sanitation/Secure Disposal
S13-005 - Cyber Incident Response Standard
S14-002 - Information Classification Standard
S14-003 - Information Security Controls
S14-006 - Authentication Tokens Standard
S14-007 - NYS Encryption Standard

S14-010 - Remote Access
NIST Federal Information Processing Standard (FIPS) Publication 140-2
NIST Federal Information Processing Standards (FIPS) Publication 199 – Standards for Security Categorization of Federal Information and Information Systems
NIST Special Publication 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations.
NIST Special Publication 800-57, Part 1 - Recommendation for Key Management – Part 1: General
NIST Special Publication 800-088r1 - Guidelines for Media Sanitization
NIST Special Publication 800-111 - Guide to Storage Encryption Technologies for End User Devices
NIST Special Publication 800-122 - Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
NIST Special Publication 800-131A - Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths
New York State Information Security Controls Standard
New York State Risk Management Standard
Health Insurance Portability and Accountability Act of 1996

Requires implementation of Assured Workloads to meet FedRAMP Moderate compliance requirements.

CAIQ Requirement/Contractor Security:

- A Consensus Assessment Initiative Questionnaire (CAIQ) is required to be submitted by the Contractor.
- NYS ITS is retaining the right to request the CAIQ be completed annually.
- A written description of Contractor's physical/virtual security and/or internal control processes are required.
- Security Logs and Reports will need to be provided in a format communicated by NYS ITS.
- At the sole discretion of ITS, ITS may accept other audited reports in lieu of the CAIQ, provided the report meets all other requirements in this section.

The contractor warrants, covenants, and represents that it shall comply fully with all applicable ITS Information Security policies and procedures located at https://its.ny.gov/eiso/policies/security during the performance of the resulting Contract. The State may terminate the Contract if it determines that Contractor has violated a material term of this section. The terms of this section shall apply equally to Contractor, officers, agents, employees, and Subcontractors, if any. Contractor agrees that all officers, agents, employees, and Subcontractors, if any, shall be made aware of and shall agree to the terms of this section.

9. MAINTENANCE/SUPPORT

Vendor shall provide maintenance and support based on its usual commercial processes.

10. INFRASTRUCTURE SUPPORT SERVICES

Infrastructure support services that do not directly or indirectly access Data may be provided in a Follow the Sun format.

11. BUSINESS CONTINUITY/DISASTER RECOVERY (BC/DR) OPERATIONS

The Contractor must provide proof of their redundant 24x7 model including site load balancing and disaster recovery. Redundancy should span at least two highly available, secure data centers in the continental United States with a minimum of 500 miles of geographic separation. Minimum availability criteria include power supply, redundant Internet connectivity with multiple providers, fire protection, etc. Maintain full off-site back-up of operating systems, software, configurations, and any data needed to successfully recover from any hardware, software, or site failure. Disaster recovery must be tested annually.

12. AUTHENTICATION TOKENS

Authentication Tokens are required and must meet the AAL1 standard as a minimum.

13. APPLICATION PROGRAM INTERFACE (API) OR SELF ELECTRONIC PORTAL

New York State requires access to both an API and electronic portal for the purposes of accessing, downloading, and/or interacting with data within the system.

B. STATEMENT OF WORK

This is an enterprise agreement subscription and as such there is no statement of work for the contractor.

1. IMPLEMENTATION OF CLOUD SOLUTION
N/A

2. RECURRING SERVICES
The items listed in the Attachment 1.

3. TRANSFER OF DATA
N/A

Contractor cannot charge for the transfer of Data unless the charges are provided for in response to this RFQ.

C. AUTHORIZED USER TERMS AND CONDITIONS

1. DATA BREACH – REQUIRED CONTRACTOR ACTIONS
Unless otherwise provided by law, in the event of a Data Breach, the Contractor shall:
1. Notify the ITS and any potentially affected Authorized User(s), or their designated contact person(s), by telephone as soon as possible, but in no event more than 12 hours from the time the Contractor confirms the Data Breach.
2. Consult with and receive authorization from the Authorized User as to the content of any notice to affected parties prior to notifying any affected parties to whom notice of the Data Breach is required, either by statute or by the Authorized User.
3. Coordinate all communication regarding the Data Breach with the ITS and Authorized User (including possible communications with third parties).
4. Cooperate with the Authorized User, ITS and any Contractor working on behalf of the Authorized User or ITS in attempting (a) to determine the scope and cause of the breach; and (b) to prevent the future recurrence of such security breaches; and
5. Take such corrective actions that the Contractor deems necessary to contain the Data Breach. Contractor shall provide Written notice to the Authorized User as to all such corrective actions taken by the Contractor to remedy the Data Breach. Unless otherwise agreed to in the Authorized User Agreement, if Contractor is unable to complete the corrective action within the required timeframe, the remedies provided in Appendix B, Section 52, Remedies for Breach shall apply and (i) the Authorized User may contract with a third party to provide the required services until corrective actions and services resume in a manner acceptable to the Authorized User, or until the Authorized User has completed a new procurement for a replacement service system; (ii) and the Contractor will be responsible for the reasonable cost of these services during this period.

Nothing herein shall in any way (a) impair the Authorized User or OAG to bring an action against Contractor to enforce the provisions of the New York State Information Security Breach Notification Act (ISBNA) or (b) limit Contractor's liability for any violations of the ISBNA or any other applicable statutes, rules, or regulations.

2. AUTHORIZED USER ACCESS TO DATA
The Authorized User shall have access to its Data at all times, through the term of the Authorized User Agreement.

The Authorized User shall have the ability to import or export Data in piecemeal or in its entirety at the Authorized User's discretion at no charge to the Authorized User. This includes the ability for the Authorized User to import or export Data to/from other Contractors.

3. CONTRACTOR ACCESS TO DATA
The Contractor shall not copy or transfer Data unless authorized in writing by the Authorized User. In such an event the Data shall be copied and/or transferred in accordance with the provisions of this Section. Contractor shall not access any Data for any purpose other than fulfilling the service. Contractor is prohibited from Data Mining, cross tabulating, monitoring Authorized User's Data usage and/or access, or performing any other Data analytics other than those required within the Authorized User Agreement. At no time shall any Data or processes (e.g. workflow, applications, etc.), which either are owned or used by the Authorized User be copied, disclosed, or retained by the Contractor or any party related to the Contractor. Contractors are allowed to perform industry standard back-ups of Data. Documentation of back-up must be provided to the Authorized User upon request. Contractor must comply with any and all security requirements within the Authorized User Agreement.

4. SUSPENSION OF SERVICES

During any period of suspension of service, the Authorized User shall have full access to all Data at no charge. The Contractor shall not take any action to erase and/or withhold any Authorized User Data, except as directed by the Authorized User.

5. EXPIRATION OR TERMINATION OF SERVICES

Upon expiration or termination of an Authorized User Agreement, the Authorized User shall have full access to all Data for a period of 60 calendar days. During this period, the Contractor shall not take any action to erase and/or withhold any Data, except as directed by the Authorized User. An Authorized User shall have the right to specify a period more than 60 calendar days in its RFQ. There will be no additional charge to the State for this access.

6. ACCESS TO SECURITY LOGS AND REPORTS

Upon request, the Contractor shall provide access to security logs and reports to the State or Authorized User in a format as specified by the Authorized User.

7. CONTRACTOR PERFORMANCE AUDIT

The Contractor shall allow the Authorized User to assess Contractor's performance by providing any materials requested in the Authorized User including but not limited to page load times, response times, uptime, and fail over time. The Authorized User may perform this Contractor performance audit with a third party at its discretion, at the Authorized User's expense.

The Contractor shall perform an independent audit of its Data Centers, at least annually, at Contractor expense. The Contractor will provide a data owner facing audit report upon request by the Authorized User. The Contractor shall identify any confidential, trade secret, or proprietary information in accordance with Appendix B, Section 9(a), Confidential/Trade Secret Materials.

Except as otherwise provided for, all status reports and other documents produced for the State become the property of the State.

8. MODIFICATION TO CLOUD SERVICE DEPLOYMENT MODEL, SERVICE MODEL, AND/OR INITIAL FUNCTIONALITY WITHIN AN AUTHORIZED USER AGREEMENT

As Cloud services, can be flexible and dynamic, delivery mechanisms may be subject to change. This may result in changes to the deployment model, service model, functionality, or SKU. The OGS and Authorized Users require notification of any such changes to ensure security and business needs are met.

Any changes to the deployment model, service model, functionality, or SKU (e.g., PaaS to IaaS) must be provided to OGS via Appendix C - Contract Modification Procedures.

In addition, notification must be provided to the Authorized User for review and acceptance, prior to implementation. Any changes to the Authorized User Agreement will require the Authorized User to re-assess the risk mitigation methodologies and strategies and revise the Authorized User Agreement as needed.

9. BACKGROUND CHECK REQUIREMENTS

All Contractor Staff shall, prior to the commencement of any services pursuant to this RFQ, whether on or off-site, comply with all State onboarding and security clearance requirements, including training and signing certifications or agreements, required for access to NYS Confidential Information or Data or required for access to NYS Facilities or Data Centers, the preceding described, collectively, as "onboarding." This includes requirements related to the access to Regulated data, including any requirements of the State's public safety agencies, or those related to the Federal Bureau of Investigation Criminal Justice Information Services (CJIS) Security Policy (https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center).

Contractor agrees that its Contractor Staff performing services on-site at NYS Facilities or Data Centers or those with logical access to NYS Confidential Information or Data (i.e., log-in access) shall be required to undergo the same security clearances as those required of ITS employees. If not physically or virtually escorted, each Contractor Staff designated to work under the Authorized User Agreement with ITS shall submit identifying information to the State and be fingerprinted. ITS shall arrange for the scheduling of fingerprinting. Such fingerprints shall be submitted to the NYS Division of Criminal Justice Services for a state criminal history record check and, at ITS' discretion, to the Federal Bureau of Investigation for a national criminal history record check.

Contractor also agrees that its Contractor Staff performing services on-site at NYS Facilities or Data Centers may be required to comply with those health checks which NYS requires of its own employees working on-site including for example providing proof of vaccination against, and/or testing for, infectious disease such as COVID-19.

All expenses, including travel and lodging, associated with the onboarding and security clearance process including fingerprinting of Contractor Staff are the responsibility of the Contractor and are not reimbursable.

ITS shall make all suitability determinations on Contractor Staff. For purposes of this Section, a "suitability determination" is a determination that there are reasonable grounds to believe that an individual will likely be able to perform the Authorized User Agreement requirements without undue risk to the interests of the State. Failure of a security clearance or non-compliance with this Section will disqualify any Contractor Staff from performing any services on the Authorized User Agreement. If any Contractor Staff are removed from providing services under the Authorized User Agreement, they may be subject to all onboarding and security clearance requirements if they are returned to performing services under the Authorized User Agreement.

All Contractor Staff shall, at the termination of their providing services to ITS under this RFQ, comply with all State off-boarding and security procedures, including return to ITS of any physical or logical access badges or other credentials that were issued by the State and required for their access to NYS Confidential Information or Data or NYS Facilities or Data Centers.

10. ACCESS TO REGULATED DATA

The Contractor agrees to comply with the requirements listed in Appendix F for those Applicable Statutory Requirements indicated on the cover page of this RFQ. In addition to the terms found in the Contract and Appendix F, the following provisions shall apply to this RFQ.

Criminal Justice Information Services

The Contractor agrees to comply with all requirements in the most recent approved version Criminal Justice Information Services (CJIS) Security Policy, available at https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center/view and the terms of the CJIS Security Addendum below. As of the date of this RFQ, the most recent approved version of the CJIS Security Policy is Version 5.9.5, dated July 9, 2024.

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks, and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

a. Investigate or decline to investigate any report of unauthorized use.

b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer
Criminal Justice Information Services Division, FBI
1000 Custer Hollow Road
Clarksburg, West Virginia 26306

Safeguarding Federal Tax Information

I. PERFORMANCE

In performance of this Contract, the Contractor agrees to comply with and assume responsibility for compliance by Contractor Staff with the following requirements:

(1) All work will be performed under the supervision of the Contractor.

(2) The Contractor and Contractor Staff to be authorized access to Federal Tax Information (FTI) must meet the background check requirements defined in IRS Publication 1075. The Contractor will maintain a list of Contractor Staff authorized access to FTI. Such list will be provided to ITS and, upon request, to the IRS.

(3) FTI made available in any format shall be used only for the purpose of carrying out the provisions of this Contract. FTI in any format shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this Contract. Inspection by or disclosure of FTI to anyone other than the Contractor or Contractor Staff authorized is prohibited.
(4) All FTI will be accounted for upon receipt and properly stored before, during, and after processing. In addition, any related output and products will be given the same level of protection as required for the source material.
(5) The Contractor will certify that the FTI processed during the performance of this Contract will be completely purged from all physical and electronic data storage with no output to be retained by the Contractor at the time the work is completed. If immediate purging of physical and electronic data storage is not possible, the Contractor will certify that any FTI in physical or electronic storage will remain safeguarded to prevent unauthorized disclosures.
(6) Any spoilage or any intermediate hard copy printout that may result during the processing of FTI will be given to ITS. When this is not possible, the Contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts and will provide ITS with a statement containing the date of destruction, description of material destroyed, and the destruction method.
(7) All computer systems receiving, processing, storing, or transmitting FTI must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to FTI.
(8) No work involving FTI furnished under this Contract will be subcontracted without prior written approval of the IRS.
(9) Contractor will ensure that the terms of FTI safeguards described herein are included, without modification, in any approved subcontract for work involving FTI.
(10) To the extent the terms, provisions, duties, requirements, and obligations of this Contract apply to performing services with FTI, the Contractor shall assume toward the subcontractor all obligations, duties, and responsibilities that ITS under this Contract assumes toward the Contractor, and the subcontractor shall assume toward the Contractor all the same obligations, duties and responsibilities which the Contractor assumes toward ITS under this Contract.
(11) In addition to the subcontractor's obligations and duties under an approved subcontract, the terms and conditions of this Contract apply to the subcontractor, and the subcontractor is bound and obligated to the Contractor hereunder by the same terms and conditions by which the contractor is bound and obligated to ITS under this Contract.
(12) For purposes of this contract, the term "contractor" includes any officer or employee of the contractor with access to or who uses FTI, and the term "subcontractor" includes any officer or employee of the subcontractor with access to or who uses FTI.
(13) ITS will have the right to void the Contract if the Contractor fails to meet the terms of FTI safeguards described herein.

II. CRIMINAL/CIVIL SANCTIONS

(1) Each Contractor Staff of a Contractor to whom FTI is or may be disclosed shall be notified in writing that FTI disclosed to such Contractor Staff can be used only for a purpose and to the extent authorized herein, and that further disclosure of any FTI for a purpose not authorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution.
(2) Each Contractor Staff of a Contractor to whom FTI is or may be accessible shall be notified in writing that FTI accessible to such Contractor Staff may be accessed only for a purpose and to the extent authorized herein, and that access/inspection of FTI without an official need-to-know for a purpose not authorized herein constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution.
(3) Each Contractor Staff of a Contractor to whom FTI is or may be disclosed shall be notified in writing that any such unauthorized access, inspection or disclosure of FTI may also result in an award of civil damages against the Contractor Staff in an amount equal to the sum of the greater of $1,000 for each unauthorized access, inspection, or disclosure, or the sum of actual damages sustained as a result of such unauthorized access, inspection, or disclosure, plus in the case of a willful unauthorized access, inspection, or disclosure or an unauthorized access/inspection or disclosure which is the result of gross negligence, punitive damages, plus the cost of the action. These penalties are prescribed by IRC sections 7213, 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.
(4) Additionally, it is incumbent upon the Contractor to inform its Contractor Staff of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1),

which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of their employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.
(5) Granting a contractor access to FTI must be preceded by certifying that each Contractor Staff understands ITS's security policies and procedures for safeguarding FTI. The Contractor and Contractor Staff must maintain their authorization to access FTI through annual recertification of their understanding of ITS's security policy and procedures for safeguarding FTI. The initial certification and recertifications must be documented and placed in the ITS's files for review. As part of the certification and at least annually afterwards, the Contractor and each Contractor Staff must be advised of the provisions of IRC sections 7213, 7213A, and 7431 (see Exhibit 4, *Sanctions for Unauthorized Disclosure*, and Exhibit 5, *Civil Damages for Unauthorized Disclosure*). The training on ITS's security policies and procedures provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches (See Section 10). For the initial certification and the annual recertifications, the Contractor and each Contractor Staff must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. INSPECTION

The IRS and ITS, with 24-hour notice, shall have the right to send its inspectors into the offices and plants of the Contractor to inspect facilities and operations performing any work with FTI under this Contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process, or transmit FTI. Based on the inspection, corrective actions may be required in cases where the Contractor is found to be noncompliant with FTI safeguard requirements.

COMPLIANCE WITH HIPAA (HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996), HI-TECH (HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT OF 2009), AND OTHER HEALTH INFORMATION PRIVACY AND SECURITY LAWS

Definitions:
The following terms used in this Section shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information (PHI), Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

(a) Business Associate. "Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, and in this Section may refer to Contractor or its Subcontractor(s), to the extent Contractor or its Subcontractor(s) create, receive, maintain, or transmit protected health information on behalf of ITS.

(b) Covered Entity. By entering into the Contract, ITS does not affirm that it necessarily meets the definition of a "Covered Entity" or a "Business Associate" under the HIPAA statute, and rather affirms that ITS may in a given instance be acting as a "conduit" or in another capacity providing services to other entities, some of which themselves may be covered entities. But to the extent ITS is deemed to be covered by HIPAA or HI-TECH, the Parties agree the term "Covered Entity" in this Section shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103.

(c) HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

(d) "Medicaid Confidential Data" (MCD) includes all information about a Medicaid recipient or applicant, including enrollment information, eligibility data and protected health information. The NYS Department of Health (DOH) is the Single State Agency responsible for the administration of the New York State Medicaid program in New York State, including ensuring the security and confidentiality of MCD data.

HIPAA Protected Health Information Obligations and Activities of Contractor

To the extent Contractor or its Subcontractor(s) create, receive, maintain, or transmit protected health information on behalf of ITS pursuant to their responsibilities under the Contract, Contractor agrees that it is subject to, will abide by, and will require in writing its Subcontractors to similarly abide by, the following requirements applicable to Business Associates under HIPAA, agreeing to:

(a) Not use or disclose protected health information other than as permitted or required by the Contract or as required by law.

(b) Use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Contract.

(c) Report to ITS within ten (10) business days or fewer any use or disclosure of protected health information not provided for by the Contract of which it becomes aware. In no event shall Contractor exceed the timeframe for reporting to ITS breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware. Contractor shall provide ITS all information reasonably requested by ITS concerning any breach. Contractor shall also provide the following information to ITS upon first instance of the notification of breach: the identification of each individual whose unsecured protected health information has been, or is reasonably believed by Contractor, to have been, accessed, acquired, used, or disclosed during the breach.

(d) In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any Subcontractors that create, receive, maintain, or transmit protected health information on behalf of Contractor agree in writing to the same restrictions, conditions, and requirements that apply to Contractor with respect to such information.

(e) Make available protected health information in a designated record set to ITS, in a manner to be prescribed by ITS within a reasonable timeframe not to exceed fifteen (15) days, absent extenuating circumstances, as necessary to satisfy obligations which ITS or the entities it provides services to reasonably believe applicable to them under 45 CFR 164.524. In the event Contractor or its Subcontractor(s) receive any request for such protected health information directly from an individual, Contractor shall refer such request to ITS within a reasonable timeframe not to exceed ten (10) business days.

(f) Make any amendment(s) to protected health information in a designated record set as directed by ITS pursuant to 45 CFR 164.526 or take other measures as necessary to satisfy obligations that ITS reasonably believes it has under 45 CFR 164.526, in the manner as prescribed by ITS and within twenty (20) business days of such request. In the event Contractor or its Subcontractor(s) receive any request to amend a data set directly from an individual, Contractor shall refer such request to ITS within a reasonable timeframe not to exceed ten (10) business days.

(g) Maintain and make available the information required to provide an accounting of disclosures to ITS as necessary to satisfy obligations that ITS reasonably believes it has under 45 CFR 164.528, in the manner as prescribed by ITS and within ten (10) business days of such request. In the event Contractor or its Subcontractor(s) receive any request for an accounting of disclosures directly from an individual, Contractor shall refer such request to ITS within a reasonable timeframe not to exceed ten (10) business days.

(h) To the extent Contractor or its Subcontractor(s) are to carry out one or more of obligation(s) ITS may have under Subpart E of 45 CFR Part 164, in performing such obligations, comply with the requirements of Subpart E that apply to ITS; and

(i) Make either Contractor's or its Subcontractor(s)', or both's, internal practices, books, and records available to the Secretary of the Department of Health and Human Services and to ITS, for purposes of determining compliance with the HIPAA and HI-TECH Rules.

Permitted Uses and Disclosures of Protected Health Information by Contractor and its Subcontractor(s)

(a) Contractor and its Subcontractor(s) may only use or disclose protected health information as necessary to perform the services set forth in the Contract, provided however, that if de-identified information can be used in lieu of individually identifiable health information with the same effect, Contractor and its Subcontractor(s) shall use de-identified information in their performance of the Contract in accordance with 45 CFR 164.514(a)-(c).

(b) Contractor and its Subcontractor(s) may use or disclose protected health information as required by law.

(c) Contractor and its Subcontractor(s) agrees to make only those uses, disclosures and requests for protected health information that are consistent with the minimum necessary policies and procedures of ITS or the entit(ies) for whom ITS provides services which entail the creation, reception, maintenance, or transmittal of protected health information.

(d) Contractor and its Subcontractor(s) may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 except as may be provided for in the Contract or for the proper management and administration of Contractor or its Subcontractor(s), including the carrying out of the Contractor's or its Subcontractor(s)' legal responsibilities.

Other Health Information Obligations and Activities of Contractor

Contractor or its Subcontractor(s) may not disclose other types of health information protected by federal, State, or local law including but not limited to personally identifiable mental health information protected under NYS Mental Hygiene Law §33.16, other personally identifiable health information or HIV information protected under NYS Health Law sections §18 or Article 27-F, or substance abuse information protected under federal regulations 42 CFR Part 2.

Contractor or its Subcontractor(s) may not disclose Medicaid Confidential Data without the prior written approval of the New York State Department of Health (DOH), either directly or as provided to Contractor or its Subcontractor(s) through ITS. If contacted by DOH, while also informing ITS, Contractor or its Subcontractor(s) shall reasonably work with DOH to identify any individuals who may have inappropriately or unlawfully accessed Medicaid Confidential Data.

Contractor agrees to ensure that Contractor and any agent, including a Subcontractor, to whom Contractor provides Medicaid Confidential Data, agrees to the same restrictions and conditions that apply throughout the Contract. Further, Contractor agrees to state in any such agreement, contract, or document that the party to whom Contractor is providing the Medicaid Confidential Data may not further disclose it without the prior written approval of the New York State Department of Health. Contractor agrees to include the notices preceding, as well as references to statutory and regulatory citations set forth above, in any agreement, contract or document that Contractor enters into that involves Medicaid Confidential Data.

The federal Center for Medicare and Medicaid Services (CMS) requires that all contracts and/or agreements executed between the Department of Health and any second party that will receive Medicaid Confidential Data must include contract language that will bind such Parties to ensure that contractor(s) abide by the regulations and laws that govern the protection of individual, Medicaid confidential level data.

Medicaid Confidential Data includes all information about a recipient or applicant, including enrollment information, eligibility data and protected health information.

Contractor must comply with the following State and federal laws and regulations:

- Section 367b(4) of the NY Social Services Law
- New York State Social Services Law Section 369 (4)
- NYS Mental Hygiene Law §33.16,
- Article 27-F of the New York Public Health Law & 18 NYCRR 360-8.1
- Social Security Act, 42 USC 1396a (a)(7)
- Federal regulations at 42 CFR 431.302, 42 C.F.R. Part 2
- The Health Insurance Portability and Accountability act (HIPAA), at 45 CFR Parts 160 and 164

Please note that Medicaid Confidential Data released to Contractor may contain AIDS/HIV related NYS Confidential Information as defined in Section 2780(7) of the New York Public Health Law. As required by New York Public Health Law Section 2782(5), the following notice is provided to Contractor:

"This information has been disclosed to you from confidential records which are protected by state law. State law prohibits you from making any further disclosure of this information without the specific written consent of the person to whom it pertains, or as otherwise permitted by law. Any unauthorized further disclosure in violation of state law may result in a fine or jail sentence or both. A general authorization for the release of medical or other information is NOT sufficient authorization for the release for further disclosure."

Alcohol and Substance Abuse Related Confidentiality Restrictions:

Alcohol and substance abuse information is confidential pursuant to 42 C.F.R. Part 2. General authorizations are ineffective to obtain the release of such data. The federal regulations provide for a specific release for such data.

Term and Termination

(a) Termination for cause under HIPAA or HI-TECH. The Term of this Section shall be as described elsewhere in the "Term" section of the Contract. Among the other reasons for which ITS may terminate the Contract prior to the end of its Term date for cause, ITS may terminate the Contract if ITS determines the Contractor or its Subcontractor(s) have violated a material term of this HIPAA and HI-TECH Compliance Section of the Contract, and Contractor or its Subcontractor(s) have not cured the breach or ended the violation within any time that has been specified by ITS.

(b) Contractor's and its Subcontractor(s)' Obligations Upon Termination. Upon termination of the Contract for any reason, Contractor and its Subcontractor(s) shall return to ITS, transfer to another of ITS' contractors as directed by ITS, or, if agreed to by ITS on an individual case-by-case basis, destroy all protected health information received from ITS, or created, maintained, or received by the Contractor and its Subcontractor(s) on behalf of ITS, that the Contractor and its Subcontractor(s) still maintain in any form. Contractor and its Subcontractor(s) shall retain no copies of the protected health information. Contractor understands and agrees and will require of its Subcontractor(s) in writing that Contractor and its Subcontractor(s) are required to receive written approval from ITS prior to the return, transfer, or destruction of any protected health information.

(c) Survival. Contractor's and its Subcontractor(s)' obligations under this HIPAA and HI-TECH Compliance section of the Contract shall survive the termination of the Contract.

Miscellaneous

(a) Regulatory References. A reference in the Contract to a section in the HIPAA or HI-TECH Rules means the section as in effect or as amended.

(b) Amendment. The Parties agree to take such action as is necessary to amend the Contract from time to time as is necessary for compliance with the requirements of the HIPAA or HI-TECH Rules and any other applicable law.

(c) Interpretation. Any ambiguity in the Contract shall be interpreted to permit compliance with the HIPAA or HI-TECH Rules.

(d) Sub-contractors. Contractor shall require any Subcontractors that it uses that create, receive, maintain, or transmit protected health information on behalf of ITS under the Contract to conform to these HIPAA and HI-TECH Compliance requirements in addition to any other security, privacy, or applicable terms of the Contract.

D. QUESTIONS

All questions shall be emailed to the Designated Contact E-Mail Address indicated on the Cover Page of this RFQ.

Contractors are strongly encouraged to submit questions as early as possible. However, all questions must be submitted by the Question due date and time listed on the Cover Page of this RFQ. Answers to all questions of a substantive nature shall be provided to all Contractors who received this RFQ in the form of a question-and-answer document.

All Bids must conform to the terms set forth in this RFQ and the OGS Information Technology Umbrella Contract – Manufacturer Based. Extraneous terms or material deviations (including additional, inconsistent, conflicting, or alternative terms) may render the Bid non-responsive and may result in rejection of the Bid. Extraneous terms submitted on standard, pre-printed forms (including but not limited to product literature, order forms, license agreements, contracts, or other documents) that are attached or referenced with submissions shall not be considered part of the Bid or Authorized User Agreement but shall be deemed included for informational or promotional purposes only.

Each proposed extraneous term must be specifically enumerated in writing and specify the section of this RFQ that Bidder proposes to modify and the reasons why. Any extraneous terms must be submitted during the Question-and-Answer period as listed on the Cover Page of this RFQ. Extraneous terms submitted after this time will not be considered.

No extraneous term shall be incorporated into the Authorized User Agreement unless expressly accepted by ITS in writing. Acceptance and/or processing of a Bid shall not constitute acceptance of extraneous terms.

E. DOWNSTREAM PROHIBITION

None.

F. AUTHORIZED USER DISPUTE RESOLUTION PROCESS

Should a dispute or protest arise regarding this RFQ, the dispute or protest will be considered and decided by the Authorized User.

1. Disputes or Controversies Occurring During the Term of the Authorized User Agreement.
In the event there is a dispute or controversy during the term of the Authorized User Agreement resulting from this RFQ, the Contractor and Authorized User agree to exercise their best efforts to resolve the dispute as soon as possible. The Contractor and Authorized User shall, without delay, continue to perform their respective obligations under the resulting Authorized User Agreement and this Centralized Contract which are not affected by the dispute. Primary responsibility for resolving any dispute arising under the Authorized User Agreement shall rest with the persons designated by the Authorized User and the Contract's Contract Administrator and/or Account Manager.

In the event the Authorized User is dissatisfied with the Contractor's Products provided under the Authorized User Agreement, the Authorized User shall notify the Contractor in writing pursuant to the terms of the Contract. In the event the Contractor has any disputes with the Authorized User, the Contractor shall so notify the Authorized User in writing. If either party notifies the other of such dispute or controversy, the other party shall then make good faith efforts to solve the problem or settle the dispute amicably, including meeting with the party's representatives to attempt diligently to reach a satisfactory result.

If negotiation between such persons fails to resolve any such dispute to the satisfaction of the parties within fourteen (14) business days or as otherwise agreed to by the Contractor and Authorized User, of such notice, then the matter shall be submitted to the persons designated by the Authorized User and the Contractor's senior officer of the rank of Vice President or higher as its representative. Such representatives shall meet in person and shall attempt in good faith to resolve the dispute within the next fourteen (14) business days or as otherwise agreed to by the parties. This meeting must be held before either party may seek any other method of dispute resolution, including judicial or governmental resolutions. Notwithstanding the foregoing, nothing in this section shall be construed to prevent either party from seeking and obtaining temporary equitable remedies, including injunctive relief.

The Contractor shall extend the dispute resolution period for so long as the Authorized User continues to make reasonable efforts to cure the breach, except with respect to disputes about the breach of payment of fees or infringement of its or its licensors' intellectual property rights.

G. RESERVED RIGHTS

Bidders are hereby notified that New York State reserves the right to:

1. Reject any or all Bids received in response to the solicitation.
2. Withdraw the solicitation at any time, at the Agency's sole discretion.
3. Make an award under the solicitation in whole or in part.
4. Disqualify any Bidder whose conduct and/or Bid fails to conform to the requirements of the solicitation.
5. Seek clarifications and revisions of Bids.
6. Prior to the Bid deadline, amend the solicitation requirements to correct errors or oversights, or to supply additional information, as it becomes available.
7. Prior to the Bid deadline, direct Bidders to submit Bid modifications addressing subsequent solicitation amendments.
8. Change any of the schedule dates with timely notification to all prospective Bidders.
9. Eliminate any mandatory, non-material specifications that cannot be complied with by all of the prospective Bidders.
10. Waive any requirements that are not material.
11. Utilize any and all ideas submitted in the Bids received.
12. Negotiate with the Bidder responding to the solicitation within the solicitation requirements to serve the best interests of the State. This includes requesting increased discounts and clarifications of any or all Bidder's' Bids.
13. Require clarification at any time during the procurement process and/or require correction of arithmetic or other apparent errors for the purpose of assuring a full and complete understanding of a Bidder's Bid and/or to determine a Bidder's compliance with the requirements of the solicitation; and
14. Select and award to other than the selected Bidder(s) in the event of unsuccessful negotiations or, optionally, in other specified circumstances as detailed in the solicitation requirements.

15. Purchase none, some, all or more of the quantities of the items listed in Attachment 1 under this RFQ.
16. If applicable, consultants will be required to comply with ITS policies and procedures; pass background checks; and sign non-disclosure agreements.
17. If applicable, vendors may be required to complete Form A – Consultant Disclosure Form.
18. Extend the term of this agreement in accordance with the above outlined solicitation.

Manufacturer / Authorized Reseller Information

This Page is to be Completed By the Manufacturer or Authorized Reseller Responding to the RFQ

The RFQ Response must be fully and properly executed by an authorized person. By signing you certify your express authority to sign on behalf of yourself, your company, or other entity and full knowledge and acceptance of this RFQ (including any Questions/Answers or addenda), the OGS Centralized Contract and that all information provided is complete, true and accurate. Quotes received by RFQ due date/time are binding and non-retractable for 120 days or as stipulated in the RFQ.

Contract #	Manufacturer Name	Authorized Reseller Name
PM67982	Google	ThunderCat Technology, LLC

Manufacturer or Reseller Signature: Jean Kim Digitally signed by Jean Kim Date: 2024.11.04 08:07:56 -05'00' *Date:* 11/04/2024	*Phone Number:* 703-568-3378 *E-Mail:* kstokley@thundercattech.com
Printed or Typed Name: Jean Kim	*Title:* Contracts

If you are not providing a RFQ Response, place an "x" in the box, please explain why you are not responding, and return this page only.

☐ WE ARE UNABLE TO RESPOND AT THIS TIME BECAUSE:

After fully completing the information above, please submit this page via e-mail with "Request for Quote – Financial Response – Cloud Solution" (Excel) to the Authorized User indicated on the Cover Page. Authorized User reserves the right to request the original executed page of this RFQ.

NON-COLLUSIVE BIDDING CERTIFICATION REQUIRED BY SECTION 139-D OF THE STATE FINANCE LAW

SECTION 139-D, Statement of Non-Collusion in bids to the State:

BY SUBMISSION OF THIS BID, BIDDER AND EACH PERSON SIGNING ON BEHALF OF BIDDER CERTIFIES, AND IN THE CASE OF JOINT BID, EACH PARTY THERETO CERTIFIES AS TO ITS OWN ORGANIZATION, UNDER PENALTY OF PERJURY, THAT TO THE BEST OF HIS/HER KNOWLEDGE AND BELIEF:

[1] The prices of this bid have been arrived at independently, without collusion, consultation, communication, or agreement, for the purposes of restricting competition, as to any matter relating to such prices with any other Bidder or with any competitor;

[2] Unless otherwise required by law, the prices which have been quoted in this bid have not been knowingly disclosed by the Bidder and will not knowingly be disclosed by the Bidder prior to opening, directly or indirectly, to any other Bidder or to any competitor; and

[3] No attempt has been made or will be made by the Bidder to induce any other person, partnership or corporation to submit or not to submit a bid for the purpose of restricting competition.

A BID SHALL NOT BE CONSIDERED FOR AWARD NOR SHALL ANY AWARD BE MADE WHERE [1], [2], [3] ABOVE HAVE NOT BEEN COMPLIED WITH; PROVIDED HOWEVER, THAT IF IN ANY CASE THE BIDDER(S) CANNOT MAKE THE FOREGOING CERTIFICATION, THE BIDDER SHALL SO STATE AND SHALL FURNISH BELOW A SIGNED STATEMENT WHICH SETS FORTH IN DETAIL THE REASONS THEREFORE:

Subscribed to under penalty of perjury under the laws of the State of New York, this 4th day of November, 2024 as the act and deed of said corporation of partnership.

STATE OF NEW YORK }

} SS

COUNTY OF Loudoun }

On the 4th day of November in the year of 2024, before me personally appeared Jean Kim, personally known to me or proved to me on the basis of satisfactory evidence to be the individual whose name is subscribed to the foregoing Non-collusive Bidding Certification (instrument) and acknowledged to me that he/she executed the same in his/her capacity, and on his/her own behalf.

Notary Public Caitlin T. Herring

Registration No: 7961259

CAITLIN TAYANNA HERRING
NOTARY PUBLIC
REG. #7961259
MY COMMISSION EXPIRES
03/31/2025
COMMONWEALTH OF VIRGINIA

IF BIDDER(S) (ARE) A PARTNERSHIP, COMPLETE THE FOLLOWING:

NAMES OF PARTNERS OR PRINCIPALS	LEGAL RESIDENCE

IF BIDDER(S) (ARE) A CORPORATION, COMPLETE THE FOLLOWING:

NAME

Thomas Deierlein

President:
Thomas Deierlein

Secretary:
Matthew Smith

Treasurer:

LEGAL RESIDENCE

[redacted]

Identifying Data

Potential Contractor ThunderCat Technology, LLC

Address 11190 Sunrise Valley Drive, Suite 200
Street
Reston, VA 20191
City, Town, etc.

Telephone 703-674-0216 (If applicable, Responsible Corporate Officer)

Name Jean Kim Title Contracts

Signature

Joint or combined bids by companies or firms must be certified on behalf of each participant.

Legal name of person, firm or corporation	Legal name of person, firm or corporation
By	
Name	Name
Title	Title
Address	Address
Street	Street
City State	City State

Google Cloud Master Terms
The Google Cloud Master Terms are comprised of the Google Cloud Master General Terms ("General Terms"), and all Services Schedules and Order Forms that are incorporated by reference into the General Terms (collectively, the "Terms"). The Terms are applicable in conjunction with the terms of the New York State ("NYS") Statewide - Information Technology Umbrella Contract – Manufacturer Based ("PM67982"), which serves as the procurement vehicle herein. The attached Google Cloud Platform Services Schedule ("Services Schedule") is thus incorporated herein by reference and applicable to the Services.

Google Cloud Master General Terms
1. Services. After Customer and Reseller and/or Distributor complete and execute an Order Form, (a) Google will provide the Services to Customer in accordance with these Terms, including the SLAs, and (b) Customer may use the Services in accordance with the terms that made up these Terms.

2. Customer Obligations.
2.1 Consents. Customer is responsible for any consents and notices required to permit (a) Customer's use and receipt of the Services and (b) Google's accessing, storing, and processing of data provided by Customer (including Customer Data, if applicable) under the Terms.

2.2 Compliance. Customer will (a) ensure that Customer and its End Users' use of the Services complies with the Terms, (b) use commercially reasonable efforts to prevent and terminate any unauthorized access or use of the Services, and (c) promptly notify Google of any unauthorized use of, or access to, the Services of which Customer becomes aware.

2.3 Use Restrictions. Customer will not, and will not allow End Users to, (a) copy, modify, create a derivative work of, reverse engineer, decompile, translate, disassemble, or otherwise attempt to extract any of the source code of the Services (except to the extent such restriction is expressly prohibited by applicable law); (b) sell, resell, sublicense, transfer, or distribute the Services; or (c) access or use the Services (i) in a manner intended to avoid incurring Fees; (ii) for materials or activities that are subject to the International Traffic in Arms Regulations (ITAR) maintained by the United States Department of State; (iii) in a manner that breaches, or causes the breach of, Export Control Laws; or (iv) to transmit, store, or process health information subject to United States HIPAA regulations except as permitted by an executed HIPAA BAA with Google's Reseller or Distributor.

3. RESERVED

4. Intellectual Property.
4.1 Intellectual Property Rights. Except as expressly described in the Terms, the Terms do not grant either party any rights, implied or otherwise, to the other's content or Intellectual Property. As between the parties, Customer retains all Intellectual Property Rights in Customer Data and Customer Applications, and Google retains all Intellectual Property Rights in the Services and Software.

4.2 Feedback. [Intentionally Omitted]

5. Confidentiality. See, Base Contract, Section 2.63 of PM67982 and Appendix B, Section 65(h), of PM67982

6. Marketing and Publicity. See, Appendix B, Section 13 of PM67982

7. RESERVED

8. Warranty. See, Appendix B, Section 59 of PM67982

9. Indemnification.
9.1 Google Indemnification Obligations. See, Appendix B, Sections 61 and 62 of PM67982

9.2 Customer Intellectual Property Infringement. If Google is damaged or becomes subject to a Third-Party Legal Proceeding as a result of Customer's infringement of any third-party intellectual property, Google will pursue available remedies under applicable federal, state, or local law.

10. Liability. See, Appendix B, Section 63, 63A, and 63B of PM67982.

11. Term and Termination. See, Appendix B, Section 47 of PM67982.

12. Miscellaneous.

12.1 Notices. Google will provide notices under the Terms to Customer by sending an email to the Notification Email Address. Customer will provide notices under the Terms to Google by sending an email to legal-notices@google.com. Notice will be treated as received when the email is sent. Customer is responsible for keeping its Notification Email Address current throughout the Term.

12.2 Emails. [Intentionally Omitted]

12.3 RESERVED.

12.4 RESERVED.

12.5 Force Majeure. See, Appendix B, Section 48 of PM67982.

12.6 Subcontracting. Google may subcontract obligations under the Terms but will remain liable to Customer for any subcontracted obligations.

12.7 No Agency. These Terms do not create any agency, partnership, or joint venture between the parties.

12.8 No Waiver. Neither party will be treated as having waived any rights by not exercising (or delaying the exercise of) any rights under the Terms.

12.9 Severability. See, Base Contract, Section 2.56 of PM67982.

12.10 No Third-Party Beneficiaries. The Terms do not confer any rights or benefits to any third party unless it expressly states that it does.

12.11 Equitable Relief. Nothing in the Terms will limit either party's ability to seek equitable relief.

12.12 RESERVED.

12.13 Amendments. Except as specifically described otherwise in the Terms, any amendment to the Terms must be in writing, expressly state that it is amending the Terms.

12.14 Independent Development. Nothing in the Terms will be construed to limit or restrict either party from independently developing, providing, or acquiring any materials, services, products, programs, or technology that are similar to the subject of the Terms, provided that the party does not breach its obligations under the Terms in doing so.

12.15 RESERVED.

12.16 Conflicting Terms. These Terms are subject to and subordinate to: (1) Appendix A – Standard Clauses for New York State Contracts (2014) and reconciled to apply in conjunction with the following: (2) Base Contract of PM67982; (3) Appendix B – 22802 – Information Technology Umbrella Contract – Manufacturer Based (Statewide) General Specifications to of PM67982 (2017); and (4) all other Appendices (C,D.1,E,F,G,H,I, and J) to PM67982.

12.17 RESERVED.

12.18 RESERVED.

12.19 RESERVED.

12.20 Headers. Headings and captions used in the Terms are for reference purposes only and will not have any effect on the interpretation of the Terms.

13. Definitions.

"Affiliate" means any entity that directly or indirectly Controls, is Controlled by, or is under common Control with a party.
"AUP" means Google's acceptable use policy as defined in the applicable Services Schedule.
"BAA" or "Business Associate Agreement" is an amendment to the Customer's Reseller Agreement or Distributor Agreement, and covers the handling of Protected Health Information (as defined in HIPAA).
"Brand Features" means each party's trade names, trademarks, logos, domain names, and other distinctive brand features.
"Confidential Information" means information that one party (or an Affiliate) discloses to the other party under these Terms, and that is marked as confidential or would normally be considered confidential information under the circumstances. Customer Data is Customer's

Confidential Information. Confidential Information does not include information that is independently developed by the recipient, is shared with the recipient by a third party without confidentiality obligations, or is or becomes public through no fault of the recipient.
"Control" means control of greater than 50% of the voting rights or equity interests of a party.
"Customer Application" has the meaning described in the Services Schedule.
"Customer Data" has the meaning described in the Services Schedule (if applicable).
"Distributor" means an entity authorized by Google to distribute the Services to a Reseller for resale to federal, state, or local government entities of the United States (or representatives of such entities).
"Distributor Agreement" means, if applicable, the separate agreement between Customer and Distributor regarding the Services. The Distributor Agreement is independent of and outside the scope of these Terms.
"Customer Materials" has the meaning described in the applicable Services Schedule.
"End User" or "Customer End User" means an individual that Customer permits to use the Services or a Customer Application.
"Export Control Laws" means all applicable export and re-export control laws and regulations, including (i) the Export Administration Regulations ("EAR") maintained by the U.S. Department of Commerce, (ii) trade and economic sanctions maintained by the U.S. Treasury Department's Office of Foreign Assets Control, and (iii) the International Traffic in Arms Regulations ("ITAR") maintained by the U.S. Department of State.
"Fees" means the product of the amount of Services used or ordered by Customer multiplied by the Prices, plus any applicable Taxes. Fees will be described in Customer's Reseller Agreement or Distributor Agreement.
"Google Indemnified Materials" has the meaning described in the applicable Services Schedule.
"High Risk Activities" means activities where the failure of the Services could lead to death, serious personal injury, or severe environmental or property damage.
"HIPAA" means the Health Insurance Portability and Accountability Act of 1996 as it may be amended from time to time, and any regulations issued under it.
"Including" means including but not limited to.
"Indemnified Liabilities" means any (i) settlement amounts approved by the Customer, and (ii) damages and costs finally awarded against the Customer by a court of competent jurisdiction.
"Intellectual Property" or "IP" means anything protectable by an Intellectual Property Right.
"Intellectual Property Right(s)" means all patent rights, copyrights, trademark rights, rights in trade secrets (if any), design rights, database rights, domain name rights, moral rights, and any other intellectual property rights (registered or unregistered) throughout the world.
"Legal Process" means an information disclosure request made under law, governmental regulation, court order, subpoena, warrant, governmental regulatory or agency request, or other valid legal authority, legal procedure, or similar process.
"Liability" means any liability, whether under contract, tort (including negligence), or otherwise, regardless of whether foreseeable or contemplated by the parties.
"Notification Email Address" has the meaning described in the applicable Services Schedule.
"Order Form" has the meaning described in the applicable Services Schedule or, as applicable, an Order Form provided by a Reseller or Distributor.
"Order Term" means the period of time starting on the Services Start Date for the Services and continuing for the period indicated on the Order Form unless terminated in accordance with the Terms.
"Reseller Agreement" means the separate agreement between Customer and Reseller regarding the Services. The Reseller Agreement is independent of and outside the scope of these Terms.
"Reseller" means, if applicable, the authorized non-Affiliate third party reseller that sells Google Services through a Distributor to Customer.
"Prices" means those prices listed in the applicable Reseller Agreement or Distributor Agreement.
"Service Level Agreement" or "SLA" has the meaning described in the Services Schedule.
"Services" has the meaning described in the applicable Services Schedule.
"Services Schedule(s)" means a schedule to the Terms with terms that apply only to the services and software (if applicable) described in that schedule.
"Services Start Date" means either the start date described in the Order Form or, if none is specified in the Order Form, the date Google makes the Services available to Customer.
"Software" has the meaning described in the Services Schedule (if applicable).
"Suspend" or "Suspension" means disabling access to or use of the Services or components of the Services.
"Term" means the Term as described in the applicable Reseller Agreement or Distributor Agreement.
"Third-Party Legal Proceeding" means any formal legal proceeding filed by an unaffiliated third party before a court or government tribunal (including any appellate proceeding).
"Trademark Guidelines" means Google's Brand Terms and Conditions described at https://www.google.com/permissions/trademark/brand-terms.html.
"URL" means a uniform resource locator address to a site on the internet.
"URL Terms" has the meaning described in the Services Schedule.
"Use Restrictions" means the restrictions in Section 2.3 (Use Restrictions) of these General Terms and any additional restrictions on the use of Services described in a section entitled "Additional Use Restrictions" in the applicable Services Schedule.

G Suite Services Schedule

This G Suite Services Schedule (the "Services Schedule") supplements and is incorporated by reference into the Google Cloud Master Terms. This Services Schedule applies solely to the services described in this Services Schedule and is effective so long as there is an active Order Form. Terms defined in the General Terms apply to this Services Schedule.

1. Using the Services.

1.1 Admin Console. Google will provide Customer access to the Admin Console through which Customer may manage its use of the Services. Customer may specify one or more Administrators through the Admin Console who will have the right to access Admin Accounts. Customer is responsible for (a) maintaining the confidentiality and security of the End User Accounts and associated passwords and (b) any use of the End User Accounts. Customer agrees that Google's responsibilities do not extend to the internal management or administration of the Services for Customer.

1.2 Additional Use Restrictions. Unless otherwise permitted in the G Suite Service Specific Terms, Customer will not use, and will not allow End Users to use, the Services to place or receive emergency services calls.

1.3 Requesting Additional End User Accounts During Order Term. Customer may purchase additional End User Accounts during an Order Term by (a) executing an additional Order Form reflecting the purchase or (b) ordering End User Accounts via the Admin Console.

2. Data Processing and Security.

2.1 Data Processing Amendment. The Data Processing Amendment is incorporated into this Services Schedule once Customer accepts it in the Admin Console. If the processing of Personal Data under the Terms is subject to the GDPR, then Customer will accept the Data Processing Amendment in the Admin Console.

2.2 Updates to Data Processing Amendment. Google may only change the Data Processing Amendment where such change is required to comply with applicable law, applicable regulation, court order, or guidance issued by a governmental regulator or agency, where such change is expressly permitted by the Data Processing Amendment, or where such change meets all of the following requirements:

(a) the change is commercially reasonable;

(b) the change does not result in a degradation of the overall security of the Services;

(c) the change does not expand the scope of or remove any restrictions on Google's processing as described in Section 5.2 (Scope of Processing) of the Data Processing Amendment; and

(d) the change does not otherwise have a material adverse impact on Customer's rights under the Data Processing Amendment.

If Google makes a material change to the Data Processing Amendment in accordance with this Section 2.2, Google will notify Customer.

3. Additional Payment Terms.

3.1 Usage and Invoicing. Customer will pay all Fees for the Services and such payment will be made pursuant to the Reseller Agreement or Distributor Agreement. Google's measurement tools will be used to determine Customer's usage of the Services. Unless otherwise provided in an Order Form or required by law, Fees for Services are nonrefundable.

3.2 RESERVED.

4. Modifications.

4.1 Modifications to URL Terms. Google may change the URL Terms, subject to the following:

(a) Notification of Material Changes. Google will notify Customer of any material change to the URL Terms.

(b) When Changes Take Effect. Material changes to the URL Terms will become effective 30 days after notice is given, except that (i) materially adverse SLA changes will become effective 90 days after notice is given and (ii) changes applicable to new Services or functionality, or required by a court order or applicable law, will be effective immediately.

(c) Objection to Changes.

(i) If a change to the URL Terms (other than as described in Section 4.1(b)(ii)) has a material adverse impact on Customer, then Customer may object to the change by notifying Google within 30 days after Google provides notice.

(ii) If Customer so notifies Google, then Customer will remain governed by the URL Terms in effect immediately before the change until the earlier of (1) the end of the then-current Order Term or (2) 12 months after the notice was given.

4.2 Modifications to Services.

(a) Deprecation Policy. Google will notify Customer at least 12 months before a Significant Deprecation unless Google reasonably determines that (i) Google is not permitted to do so by law or by contract (including if there is a change in applicable law or contract) or (ii) continuing to provide the Service that is subject to the Significant Deprecation could create a security risk or substantial economic or technical burden.

(b) Other Modifications. Subject to Section 4.2(a) (Deprecation Policy), Google may make changes to the Services, which may include adding, updating, or discontinuing any Services or portion or feature(s) of the Services. Google will notify Customer of any material change to the Core Services.

5. Temporary Suspension.

5.1 Limitations on Services Suspension. Google may Suspend Services as described in Sections 5.2 (AUP Breaches) and 5.3 (Emergency Suspension). Any Suspension under those Sections will be to the minimum extent and for the shortest duration required to (a) prevent or terminate the offending use, (b) prevent or resolve the Emergency Security Issue, or (c) comply with applicable law.

5.2 AUP Breaches. If Google becomes aware that Customer's or any End User's use of the Services breaches the AUP, Google will request that Customer correct the breach. If Customer fails to correct such breach within 24 hours of such request, or if Google is otherwise required by applicable law to take action, then Google may Suspend Services.

5.3 Emergency Suspension. Google may immediately Suspend Customer's use of the Services or an End User Account if (a) there is an Emergency Security Issue, or (b) Google is required to Suspend such use to comply with applicable law. At Customer's request, unless prohibited by applicable law, Google will notify Customer of the basis for the Suspension as soon as is reasonably possible. For Suspensions of End User Accounts, Google will provide Customer's Administrator the ability to restore End User Accounts in certain circumstances.

6. Technical Support. Google will provide G Suite Technical Support Services to Customer during the Order Term in accordance with the G Suite Technical Support Services Guidelines.

7. Additional Customer Responsibilities.

7.1 Customer Domain Name Ownership. Customer is responsible for obtaining and maintaining any rights necessary for Customer's and Google's use of the Customer Domain Names under the Terms. Before providing the Services, Google may require that Customer verify that Customer owns or controls the Customer Domain Names. If Customer does not own or control the Customer Domain Names, then Google will have no obligation to provide the Services to Customer.

7.2 Abuse Monitoring. Customer is solely responsible for monitoring, responding to, and otherwise processing emails sent to the "abuse" and "postmaster" aliases for Customer Domain Names, but Google may monitor emails sent to these aliases to allow Google to identify Services abuse.

8. Using Brand Features Within the Services. Google will display only those Customer Brand Features that Customer authorizes Google to display by uploading them into the Services. Google will display those Customer Brand Features within designated areas of the web pages displaying the Services to End Users. Customer may specify the nature of this use in the Admin Console. Google may also display Google Brand Features on such web pages to indicate that the Services are provided by Google.

9. Additional Products. Google makes optional Additional Products available to Customer and its End Users. Customer's use of Additional Products is subject to the Additional Product Terms.

10. Reseller Orders. This Section applies if Customer orders the Services from a Reseller under a Reseller Agreement.

10.1 Orders. If Customer orders Services from Reseller, then (a) fees for the Services will be set between Customer and Reseller, and any payments will be made directly to Reseller under the Reseller Agreement; (b) RESERVED (c) Customer will receive applicable SLA credits (if any) from Reseller; (d) Google may share Customer Confidential Information with Reseller as a Delegate subject to General Terms Section 5.1 (Confidentiality Obligations); and (e) Customer may request additional End User Accounts during the Order Term by contacting Reseller.

10.2 Reseller as Administrator. At Customer's discretion, Reseller may access Customer's Account or Customer's End User Accounts. As between Google and Customer, Customer is solely responsible for (a) any access by Reseller to Customer's Account or Customer's End User Accounts and (b) defining in the Reseller Agreement any rights or obligations as between Reseller and Customer with respect to the Services.

10.3 Reseller Verification of Domain Names. Reseller may verify that Customer owns or controls the Customer Domain Names. If Customer does not own or control the Customer Domain Names, then Google will have no obligation to provide the Services to Customer.

10.4 Reseller Technical Support. Customer acknowledges and agrees that Reseller may disclose End User Personal Data to Google as reasonably required in order for Reseller to handle any support issues that Customer escalates to or via Reseller.

11. Termination of Previous Agreements. If Google and Customer have previously entered into a G Suite Agreement, then that agreement will terminate on the Services Start Date, and the Agreement will govern the provision and use of the Services going forward.

12. Additional Definitions.

"Additional Products" means products, services, and applications that are not part of the Services but may be accessible for use in conjunction with the Services.

"Additional Product Terms" means the then-current terms at https://gsuite.google.com/intl/en/terms/additional_services.html.

"Admin Account" means a type of End User Account that Customer (or Reseller, if applicable) may use to administer the Services.
"Admin Console" means the online console(s) and tool(s) provided by Google to Customer for administering (i) the Services under this Services Schedule and (ii) the services set out in a Complementary Product Services Summary (if applicable).
"Administrator" means Customer-designated personnel who administer the Services to End Users on Customer's behalf, and have the ability to access Customer End User Accounts. Such access includes the ability to access, monitor, use, modify, withhold, or disclose any data available to End Users associated with their End User Accounts.
"AUP" means the then-current acceptable use policy for the Services described at https://cloud.google.com/terms/aup/.
"Complementary Product Services Summary" has the meaning given in the Data Processing Amendment.
"Core Services" means the then-current "Core Services for G Suite" as described in the Services Summary at https://gsuite.google.com/terms/user_features.html.
"Customer Data" means data submitted, stored, sent, or received via the Services by Customer or its End Users.
"Customer Domain Name" means a domain name specified in the Order Form to be used in connection with the Services.
"Customer Materials" means Customer Data and Customer Brand Features.
"Data Processing Amendment" means the then-current terms describing data protection and processing obligations with respect to Customer Data, as described at https://gsuite.google.com/terms/dpa_terms.html.
"Emergency Security Issue" means either (a) Customer's or an End User's use of the Services in breach of the AUP, where such use could disrupt (i) the Services, (ii) other customers' or their customer end users' use of the Services, or (iii) the Google network or servers used to provide the Services; or (b) unauthorized third-party access to the Services.
"End User Account" means a Google-hosted account established by Customer through the Services for an End User to use the Services.
"GDPR" has the meaning given to it in the Data Processing Amendment.
"Google Indemnified Materials" means Google's technology used to provide the Services and Google's Brand Features.
"G Suite Service Specific Terms" means the then-current terms specific to one or more Services described at https://gsuite.google.com/terms/service-terms/.
"G Suite Technical Support Services" or "TSS" means the technical support service provided by Google to Customer under the G Suite Technical Support Services Guidelines.
"G Suite Technical Support Services Guidelines" or "TSS Guidelines" means the then-current G Suite support service guidelines described at https://gsuite.google.com/terms/tssg.html.
"Notification Email Address" means the email address(es) designated by Customer in the Admin Console.
"Order Form" means the order form issued by the Reseller and/or Distributor and executed by Customer and the Reseller and/or Distributor.
"Other Services" means the then-current "Other Services for G Suite" as described in the Services Summary at https://gsuite.google.com/terms/user_features.html.
"Personal Data" has the meaning given to it in the Data Processing Amendment.
"Services" means the then-current Core Services and Other Services described at https://gsuite.google.com/terms/user_features.html.
"Significant Deprecation" means a material discontinuance of or backwards incompatible change to the Services that results in the Services no longer enabling Customer or End Users to (i) send and receive email messages; (ii) schedule and manage events; (iii) create, share, store, and synchronize files; (iv) communicate with other End Users in real time; or (v) search, archive, and export email messages.
"SLA" means the then-current service level agreement described at https://gsuite.google.com/terms/sla.html.
"URL Terms" means, as applicable, the AUP, G Suite Service Specific Terms, G Suite Technical Support Services Guidelines, and SLAs

Google: Google LLC

By:

Print: Philipp Schindler
Authorized Signatory

Title:

Date: 2020.03.12 09:36:19 -07'00'

New York State Office of Information Technology Services

By: Dennis J. Quinn

Print Name: Dennis J. Quinn

Title: Director of Contracts

Date: 3/16/2020

Request for Quote - Financial Response - Cloud Solution

RFQ Number	Authorized User Name	Contract Number	Manufacturer / Reseller Name	Date Completed	Grand Total
ITS-2024-526DB-Google Cloud SA	Information Technology Services (ITS)	PM67982	Google/ThunderCat Technology	11/4/2024	$44,513,590.03

Unanticipated Enhancements to Services is only applicable to items in Lot 4 - Implementation Services and is calculated based on the percentage the Authorized User chooses in cell E7 (not to exceed 20%).

Unanticipated Enhancements to Services (Not to Exceed 20%)	Implementation Base Total (*without* Unanticipated Enhancements)	Implementation Total (*with* Unanticipated Enhancements)	Recurring Cost Total	Data Transfer Cost Total
0%	$0.00	$0.00	$44,513,590.03	$0.00

Please See Request for Quotes for all Authorized User requirements.

Lot this RFQ Applies to: ☐ Lot 1 Software ☐ Lot 2 Hardware ☑ Lot 3 Cloud ☐ Lot 4 Implementation

If the RFQ includes Lot 4 – Implementation, Contractor must prior to submitting a response to the RFQ either hold an award for Lot 4- Implementation, or be able to provide the services under the other Lots included in the RFQ.

Instructions for When SKU's Have Been Identified by Authorized User

Authorized User will complete RFQ Number, Authorized User Name, Unanticipated Enhancements to Services Percent, Deliverable Number, Deliverable Name, Lot Number, Product Description(s), Manufacturer Part Number(s) (SKU), Net NYS Contract Price(s) and Qty, and Data Transfer Specifications in each of the three sections: Implementation Items, Recurring Items, and Data Transfer Items. The totals of each of these three sections will calculate into the Total Deliverable Cost. Please note, any anticipated deliverable travel costs are only applicable to items in Lot 4 - Implementation Services.
Manufacturer / Reseller will complete Deliverable Narrative, Additional Product Discount (Percentage), and optional Additional Product Discount (Dollars).

Instructions for When Authorized User Requires Vendor to Provide Suggested SKU's

Authorized User will complete RFQ Number and Authorized User Name, Unanticipated Enhancements to Services Percent, and Data Transfer Specifications in each of the three sections: Implementation Items, Recurring Items, and Data Transfer Items. The totals of each of these three sections will calculate into the Total Deliverable Cost. Please note, any anticipated deliverable travel costs are only applicable to items in Lot 4 - Implementation Services.
Manufacturer / Reseller will complete Deliverable Number, Deliverable Name, Deliverable Narrative, Lot Number, Product Description, Manufacturer Part Number (SKU), Net NYS Contract Price, Additional Product Discount (Percentage), Qty and optional Additional Product Discount (Dollars) to meet a

Deliverable Information

Deliverable Number	Deliverable Name

Implementation Items

RFQ Item Number	Lot Number	Product Description	Manufacturer Part Number (SKU)	Net NYS Contract Price	Additional Product Discount (Percentage)	RFQ Product Price	Qty	Additional Product Discount (Dollars)	Extended RFQ Price	Unanticipated Enhancements to Services (Not to Exceed 20%)
1										
2										
3										
4										
5										
								Anticipated Deliverable Travel Costs (Lot 4 - Implementation Services only)		$0.00
								Total Deliverable Implementation Cost	$0.00	$0.00

RFQ Number	Authorized User Name	Contract Number	Manufacturer / Reseller Name	Date Completed	Grand Total
ITS-2024-526DB-Google Cloud SA	Information Technology Services (ITS)	PM67982	Google/ThunderCat Technology	11/4/2024	$44,513,590.03

Unanticipated Enhancements to Services is only applicable to items in Lot 4 - Implementation Services and is calculated based on the percentage the Authorized User chooses in cell E7 (not to exceed 20%).

Unanticipated Enhancements to Services (Not to Exceed 20%)	Implementation Base Total (*without* Unanticipated Enhancements)	Implementation Total (*with* Unanticipated Enhancements)	Recurring Cost Total	Data Transfer Cost Total
0%	$0.00	$0.00	$44,513,590.03	$0.00

Please See Request for Quotes for all Authorized User requirements.

Recurring Items

RFQ Item Number	Lot Number	Product Description	Manufacturer Part Number (SKU)	Net NYS Contract Price	Additional Product Discount (Percentage)	RFQ Product Price	Qty	Additional Product Discount (Dollars)	Extended RFQ Price
		Year One - Term Dates to be determined							
1	Lot 3	Enterprise Agreement for Public Sector Subscription Used for a fixed price offering (not pay-as-you-go) with quantity calculated by Google up front for 1, 2, or 3 years. Prepaid with no true ups required during the 1, 2, or 3 year period covered by the fixed price. Includes unlimited Google Cloud access, but is not an aggregate of skus, and not on a per seat license basis. No professional services included. Not maintenance or support of other Google Cloud Products. Not a customer-specific sku but instead available to all public sector customers (listed on Google's Manufacturer's Price List with a list Price).							
2	Lot 3	GCP Points-Access to all GCP Solutions-Compute, Storage & Databases, Networking, Big Data Data Transfer, Machine Learning, APIs, IoT, Management, Developer and Security Tools- Payment-Monthly based Usage							
3	Lot 3	Bytes of data ingested in US for the Enterprise Plus package under subscription							
4	Lot 3	Monthly BeyondCorp Enterprise Users (Month) Qty 114,000 times 12 months = 1,368,000							
5	Lot 3	Platform Elite - Customer Hosted - Looker by Google Qty 5 times 12 months = 60							
6	Lot 3	GCP Support Base - Region 1 countries Qty 4 times 12 months = 48							
		Year Two- Term Dates to be determined							
7	Lot 3	Enterprise Agreement for Public Sector Subscription Used for a fixed price offering (not pay-as-you-go) with quantity calculated by Google up front for 1, 2, or 3 years. Prepaid with no true ups required during the 1, 2, or 3 year period covered by the fixed price. Includes unlimited Google Cloud access, but is not an aggregate of skus, and not on a per seat license basis. No professional services included. Not maintenance or support of other Google Cloud Products. Not a customer-specific sku but instead available to all public sector customers (listed on Google's Manufacturer's Price List with a list Price).							
8	Lot 3	GCP Points-Access to all GCP Solutions-Compute, Storage & Databases, Networking, Big Data Data Transfer, Machine Learning, APIs, IoT, Management, Developer and Security Tools- Payment-Monthly based Usage							
9	Lot 3	Bytes of data ingested in US for the Enterprise Plus package under subscription							
10	Lot 3	Monthly BeyondCorp Enterprise Users (Month) Qty 114,000 times 12 months = 1,368,000							
11	Lot 3	Platform Elite - Customer Hosted - Looker by Google Qty 5 times 12 months = 60							
12	Lot 3	GCP Support Base - Region 1 countries Qty 4 times 12 months = 48							
13									
14									
15									
							Total Deliverable Recurring Cost		$44,513,590.03

RFQ Number	Authorized User Name	Contract Number	Manufacturer / Reseller Name	Date Completed	Grand Total
ITS-2024-526DB-Google Cloud SA	Information Technology Services (ITS)	PM67982	Google/ThunderCat Technology	11/4/2024	$44,513,590.03

Unanticipated Enhancements to Services is only applicable to items in Lot 4 - Implementation Services and is calculated based on the percentage the Authorized User chooses in cell E7 (not to exceed 20%).	Unanticipated Enhancements to Services (Not to Exceed 20%)	Implementation Base Total (*without* Unanticipated Enhancements)	Implementation Total (*with* Unanticipated Enhancements)	Recurring Cost Total	Data Transfer Cost Total
	0%	$0.00	$0.00	$44,513,590.03	$0.00

Please See Request for Quotes for all Authorized User requirements.

Data Transfer Items

Data Transfer Specifications:

RFQ Item Number	Lot Number	Product Description	Manufacturer Part Number (SKU)	Net NYS Contract Price	Additional Product Discount (Percentage)	RFQ Product Price	Qty	Additional Product Discount (Dollars)	Extended RFQ Price	Unanticipated Enhancements to Services (Not to Exceed 20%)
1										
2										
3										
4										
5										
								Anticipated Deliverable Travel Costs (Lot 4 - Implementation Services only)		
								Total Deliverable Data Transfer Cost	$0.00	$0.00

Total Deliverable Cost	$44,513,590.03

Cover Page – Request for Quote – Cloud Solution

TO BE COMPLETED BY AUTHORIZED USER

RFQ Title **Google Cloud SA** **RFQ Number** ITS-2024-526DB

Authorized User Information:
Office of Information Technology Services
Empire State Plaza
Swan Street Building, Core 4
2nd Floor, Room 2404
Albany, NY 12223

Authorized User Delivery Information:
Joseph Marshall
NYS Office of Information Technology Services
Swan Street Bldg, Core 4, Floor 3
Empire State Plaza
Albany, NY 12227

Special Delivery Instructions:

DESIGNATED CONTACTS

Name(s)	E-Mail(s)
Dominic Brefo – Contract Manager	Its.sm.ITS_BIDS@its.ny.gov

Authorized User shall indicate if Procurement Lobbying Law/Restricted Period is in effect: ☒ **Yes** ☐ **No**
Where Procurement Lobbying Law is deemed applicable by the Authorized User, by signing, Contractor affirms that it understands and agrees to comply with the Authorized User's policies and procedures relative to permissible contacts. Information may be accessed at: Procurement Lobbying:
http://www.ogs.ny.gov/aboutOgs/regulations/defaultAdvisoryCouncil.html)

RFQ LOTS

This RFQ is for Products from the following checked Lots as defined in Award # 22802 – Information Technology Umbrella Contract – Manufacturer Based (Statewide):

☐ Lot 1 – Software ☐ Lot 2 – Hardware ☒ Lot 3 - Cloud ☐ Lot 4 – Implementation

The Authorized User named above is seeking competitive quotes from the Contractor (Manufacturer) and their Resellers (where applicable) of Information Technology Umbrella Contract – Manufacturer Based Contract(s) for the above-referenced Products. If the RFQ includes Lot 4 – Implementation, Contractor must prior to submitting a response to the RFQ either hold an award for Lot 4- Implementation or be able to provide the services under the other Lots included in the RFQ.

LOT 3 – CLOUD DATA RISK LEVEL: ☐ Low ☒ Medium ☐ High

DATA CATEGORIZATION ELEMENTS: Data is all public information.

QUESTIONS AND OTHER EVENTS

Event	Date	Time
RFQ Release Date	11/1/2024	N/A
Questions Due	11/4/2024	3:00 PM EST
Vendor Response Due Date	11/5/2024	3:00 PM EST

IS THE RFQ BIDDER POOL LIMITED TO M/WBE, SB, AND SDVOB VENDORS: ☐ Yes ☒ No

BASIS FOR AWARD
☒ Lowest Price Meeting Specified Technical Requirements
☐ Lowest Price Meeting Specified Technical Requirements **and** Mandatory Pass/Fail Requirements
☐ Best Value with Technical and Financial Score

E-RATE ELIGIBLE ☐ Yes (E-Rate Discounts are Required) ☒ No

SERVICE MODEL FOR LOT 3 – CLOUD SOLUTION *(check all that apply)*
☒ Software as a Service (SaaS)
☒ Platform as a Service (PaaS)
☒ Infrastructure as a Service(IaaS)
☐ Anything as a Service (XaaS)

DEPLOYMENT MODEL FOR LOT 3 – CLOUD SOLUTION (*Check all that apply*)	☐ Private Cloud ☐ Community Cloud ☒ Public Cloud ☐ Hybrid Cloud ☐ Other
APPLICABLE STATUTORY / POLICY REQUIRMENT	☐ None ☒ CJIS ☐ FERPA ☒ FISMA ☒ GLB ☐ HIPAA ☐ HITECH ☐ Tax ☐ PPI ☐ PCI DSS ☐ SOX ☐ ECPA ☐ Other
CAIQ REQUIRMENT	☐ Yes ☒ No
ATTACHMENTS	Attachment 1 - Request for Quote – Financial Response – Cloud Solution Attachment 2 – Non-Collusive Bidding Certification Exhibit 1 – Google Master Terms and G Suite Service Schedule

The Authorized User will not be held liable for any cost incurred by the Contractor for work performed in the preparation of a response to this RFQ or for any work performed prior to the formal execution of an Authorized User Agreement. Responses to the RFQ must be received by the deadline specified above. Contractors assume all risks for timely, properly submitted deliveries. A Contractor is strongly encouraged to arrange for delivery of RFQ responses prior to the date of the RFQ opening. LATE RFQ responses may be rejected. The received time of a RFQ response will be determined by the Authorized User.

All purchases resulting from this RFQ shall be in accordance with terms and conditions of the OGS Information Technology Umbrella Contract – Manufacturer Based Contract and any additional terms and conditions set forth in this RFQ and its Attachments.

A. SCOPE / MANDATORY REQUIREMENTS

This RFQ is being distributed to the Contractor and Resellers (where applicable) to acquire the following:

1. SCOPE

This RFQ is seeking to acquire Google cloud data acquisition, compute, cybersecurity, and support products off Office of General Services centralized Google contract PM67982. These products will be used to provide centralized IT consolidation of agency contracts, satisfy existing agency demand and result in significant savings to the state thru centralization.

The term of this agreement is two years with the option to renew based upon mutual consent. Annual purchase orders will be issued. Payment of invoices will be made for actual usage on a monthly basis.

For the duration of an Authorized User Agreement, the Cloud Solution shall conform to the Cloud Solution Manufacturer's specifications, Documentation, performance standards (including applicable license terms, warranties, guarantees, Service Level Agreements, service commitments, and credits).

2. CLOUD SERVICE MODEL

Software as a Service (SaaS)
Infrastructure as a Service (IaaS)
Platform as a Service (PaaS)

3. CLOUD DEPLOYMENT MODEL

Public Cloud (Google Cloud Platform).

4. DATA CATEGORIZATION

Risk Level: Medium. All data is public information.

5. DATA OWNERSHIP

The Authorized User shall own all right, title and interest in Data.

6. DATA LOCATION

All Data shall remain in CONUS.

7. ENCRYPTION

Contractor shall use appropriate means to preserve and protect State Data. This includes, but is not limited to, use of stable storage Media, regular data backups and archiving, password protection of volumes, and data encryption. Encryption at rest as well as Encryption in flight within the Google Cloud infrastructure. Availability to leverage CMEK (Customer Managed Encryption Keys). All Data transmitted between ITS and the Contractor must comply with NYS ITS Standard NYS-S14-007 Encryption Standard (http://its.ny.gov/document/encryption-standard).

8. SECURITY

The Contractor and its personnel shall adhere to all required compliance domains, State security policies, procedures, and directives currently existing or implemented during the term of the Contract. These compliance domains and security policies include, but are not limited to, the following New York State Information Security Policies and Standards, National Institute of Standards and Technology (NIST) Policies (or their successor policies), and statutes:

P03-002 - Information Security Policy
P08-001 - Enterprise Plan to Procure Policy
P08-005 - Accessibility of Web-Based Information and Application
S13-002 - Information Classification Standard
S13-003 - Sanitation/Secure Disposal
S13-005 - Cyber Incident Response Standard
S14-002 - Information Classification Standard
S14-003 - Information Security Controls
S14-006 - Authentication Tokens Standard
S14-007 - NYS Encryption Standard

S14-010 - Remote Access
NIST Federal Information Processing Standard (FIPS) Publication 140-2
NIST Federal Information Processing Standards (FIPS) Publication 199 – Standards for Security Categorization of Federal Information and Information Systems
NIST Special Publication 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations.
NIST Special Publication 800-57, Part 1 - Recommendation for Key Management – Part 1: General
NIST Special Publication 800-088r1 - Guidelines for Media Sanitization
NIST Special Publication 800-111 - Guide to Storage Encryption Technologies for End User Devices
NIST Special Publication 800-122 - Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
NIST Special Publication 800-131A - Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths
New York State Information Security Controls Standard
New York State Risk Management Standard
Health Insurance Portability and Accountability Act of 1996

Requires implementation of Assured Workloads to meet FedRAMP Moderate compliance requirements.

CAIQ Requirement/Contractor Security:

- A Consensus Assessment Initiative Questionnaire (CAIQ) is required to be submitted by the Contractor.
- NYS ITS is retaining the right to request the CAIQ be completed annually.
- A written description of Contractor's physical/virtual security and/or internal control processes are required.
- Security Logs and Reports will need to be provided in a format communicated by NYS ITS.
- At the sole discretion of ITS, ITS may accept other audited reports in lieu of the CAIQ, provided the report meets all other requirements in this section.

The contractor warrants, covenants, and represents that it shall comply fully with all applicable ITS Information Security policies and procedures located at https://its.ny.gov/eiso/policies/security during the performance of the resulting Contract. The State may terminate the Contract if it determines that Contractor has violated a material term of this section. The terms of this section shall apply equally to Contractor, officers, agents, employees, and Subcontractors, if any. Contractor agrees that all officers, agents, employees, and Subcontractors, if any, shall be made aware of and shall agree to the terms of this section.

9. MAINTENANCE/SUPPORT

Vendor shall provide maintenance and support based on its usual commercial processes.

10. INFRASTRUCTURE SUPPORT SERVICES

Infrastructure support services that do not directly or indirectly access Data may be provided in a Follow the Sun format.

11. BUSINESS CONTINUITY/DISASTER RECOVERY (BC/DR) OPERATIONS

The Contractor must provide proof of their redundant 24x7 model including site load balancing and disaster recovery. Redundancy should span at least two highly available, secure data centers in the continental United States with a minimum of 500 miles of geographic separation. Minimum availability criteria include power supply, redundant Internet connectivity with multiple providers, fire protection, etc. Maintain full off-site back-up of operating systems, software, configurations, and any data needed to successfully recover from any hardware, software, or site failure. Disaster recovery must be tested annually.

12. AUTHENTICATION TOKENS

Authentication Tokens are required and must meet the AAL1 standard as a minimum.

13. APPLICATION PROGRAM INTERFACE (API) OR SELF ELECTRONIC PORTAL

New York State requires access to both an API and electronic portal for the purposes of accessing, downloading, and/or interacting with data within the system.

B. STATEMENT OF WORK

This is an enterprise agreement subscription and as such there is no statement of work for the contractor.

1. IMPLEMENTATION OF CLOUD SOLUTION

N/A

2. RECURRING SERVICES

The items listed in the Attachment 1.

3. TRANSFER OF DATA

N/A

Contractor cannot charge for the transfer of Data unless the charges are provided for in response to this RFQ.

C. AUTHORIZED USER TERMS AND CONDITIONS

1. DATA BREACH – REQUIRED CONTRACTOR ACTIONS

Unless otherwise provided by law, in the event of a Data Breach, the Contractor shall:
1. Notify the ITS and any potentially affected Authorized User(s), or their designated contact person(s), by telephone as soon as possible, but in no event more than 12 hours from the time the Contractor confirms the Data Breach.
2. Consult with and receive authorization from the Authorized User as to the content of any notice to affected parties prior to notifying any affected parties to whom notice of the Data Breach is required, either by statute or by the Authorized User.
3. Coordinate all communication regarding the Data Breach with the ITS and Authorized User (including possible communications with third parties).
4. Cooperate with the Authorized User, ITS and any Contractor working on behalf of the Authorized User or ITS in attempting (a) to determine the scope and cause of the breach; and (b) to prevent the future recurrence of such security breaches; and
5. Take such corrective actions that the Contractor deems necessary to contain the Data Breach. Contractor shall provide Written notice to the Authorized User as to all such corrective actions taken by the Contractor to remedy the Data Breach. Unless otherwise agreed to in the Authorized User Agreement, if Contractor is unable to complete the corrective action within the required timeframe, the remedies provided in Appendix B, Section 52, Remedies for Breach shall apply and (i) the Authorized User may contract with a third party to provide the required services until corrective actions and services resume in a manner acceptable to the Authorized User, or until the Authorized User has completed a new procurement for a replacement service system; (ii) and the Contractor will be responsible for the reasonable cost of these services during this period.

Nothing herein shall in any way (a) impair the Authorized User or OAG to bring an action against Contractor to enforce the provisions of the New York State Information Security Breach Notification Act (ISBNA) or (b) limit Contractor's liability for any violations of the ISBNA or any other applicable statutes, rules, or regulations.

2. AUTHORIZED USER ACCESS TO DATA

The Authorized User shall have access to its Data at all times, through the term of the Authorized User Agreement.

The Authorized User shall have the ability to import or export Data in piecemeal or in its entirety at the Authorized User's discretion at no charge to the Authorized User. This includes the ability for the Authorized User to import or export Data to/from other Contractors.

3. CONTRACTOR ACCESS TO DATA

The Contractor shall not copy or transfer Data unless authorized in writing by the Authorized User. In such an event the Data shall be copied and/or transferred in accordance with the provisions of this Section. Contractor shall not access any Data for any purpose other than fulfilling the service. Contractor is prohibited from Data Mining, cross tabulating, monitoring Authorized User's Data usage and/or access, or performing any other Data analytics other than those required within the Authorized User Agreement. At no time shall any Data or processes (e.g. workflow, applications, etc.), which either are owned or used by the Authorized User be copied, disclosed, or retained by the Contractor or any party related to the Contractor. Contractors are allowed to perform industry standard back-ups of Data. Documentation of back-up must be provided to the Authorized User upon request. Contractor must comply with any and all security requirements within the Authorized User Agreement.

4. SUSPENSION OF SERVICES

During any period of suspension of service, the Authorized User shall have full access to all Data at no charge. The Contractor shall not take any action to erase and/or withhold any Authorized User Data, except as directed by the Authorized User.

5. EXPIRATION OR TERMINATION OF SERVICES

Upon expiration or termination of an Authorized User Agreement, the Authorized User shall have full access to all Data for a period of 60 calendar days. During this period, the Contractor shall not take any action to erase and/or withhold any Data, except as directed by the Authorized User. An Authorized User shall have the right to specify a period more than 60 calendar days in its RFQ. There will be no additional charge to the State for this access.

6. ACCESS TO SECURITY LOGS AND REPORTS

Upon request, the Contractor shall provide access to security logs and reports to the State or Authorized User in a format as specified by the Authorized User.

7. CONTRACTOR PERFORMANCE AUDIT

The Contractor shall allow the Authorized User to assess Contractor's performance by providing any materials requested in the Authorized User including but not limited to page load times, response times, uptime, and fail over time. The Authorized User may perform this Contractor performance audit with a third party at its discretion, at the Authorized User's expense.

The Contractor shall perform an independent audit of its Data Centers, at least annually, at Contractor expense. The Contractor will provide a data owner facing audit report upon request by the Authorized User. The Contractor shall identify any confidential, trade secret, or proprietary information in accordance with Appendix B, Section 9(a), Confidential/Trade Secret Materials.

Except as otherwise provided for, all status reports and other documents produced for the State become the property of the State.

8. MODIFICATION TO CLOUD SERVICE DEPLOYMENT MODEL, SERVICE MODEL, AND/OR INITIAL FUNCTIONALITY WITHIN AN AUTHORIZED USER AGREEMENT

As Cloud services, can be flexible and dynamic, delivery mechanisms may be subject to change. This may result in changes to the deployment model, service model, functionality, or SKU. The OGS and Authorized Users require notification of any such changes to ensure security and business needs are met.

Any changes to the deployment model, service model, functionality, or SKU (e.g., PaaS to IaaS) must be provided to OGS via Appendix C - Contract Modification Procedures.

In addition, notification must be provided to the Authorized User for review and acceptance, prior to implementation. Any changes to the Authorized User Agreement will require the Authorized User to re-assess the risk mitigation methodologies and strategies and revise the Authorized User Agreement as needed.

9. BACKGROUND CHECK REQUIREMENTS

All Contractor Staff shall, prior to the commencement of any services pursuant to this RFQ, whether on or off-site, comply with all State onboarding and security clearance requirements, including training and signing certifications or agreements, required for access to NYS Confidential Information or Data or required for access to NYS Facilities or Data Centers, the preceding described, collectively, as "onboarding." This includes requirements related to the access to Regulated data, including any requirements of the State's public safety agencies, or those related to the Federal Bureau of Investigation Criminal Justice Information Services (CJIS) Security Policy (https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center).

Contractor agrees that its Contractor Staff performing services on-site at NYS Facilities or Data Centers or those with logical access to NYS Confidential Information or Data (i.e., log-in access) shall be required to undergo the same security clearances as those required of ITS employees. If not physically or virtually escorted, each Contractor Staff designated to work under the Authorized User Agreement with ITS shall submit identifying information to the State and be fingerprinted. ITS shall arrange for the scheduling of fingerprinting. Such fingerprints shall be submitted to the NYS Division of Criminal Justice Services for a state criminal history record check and, at ITS' discretion, to the Federal Bureau of Investigation for a national criminal history record check.

Contractor also agrees that its Contractor Staff performing services on-site at NYS Facilities or Data Centers may be required to comply with those health checks which NYS requires of its own employees working on-site including for example providing proof of vaccination against, and/or testing for, infectious disease such as COVID-19.

All expenses, including travel and lodging, associated with the onboarding and security clearance process including fingerprinting of Contractor Staff are the responsibility of the Contractor and are not reimbursable.

ITS shall make all suitability determinations on Contractor Staff. For purposes of this Section, a "suitability determination" is a determination that there are reasonable grounds to believe that an individual will likely be able to perform the Authorized User Agreement requirements without undue risk to the interests of the State. Failure of a security clearance or non-compliance with this Section will disqualify any Contractor Staff from performing any services on the Authorized User Agreement. If any Contractor Staff are removed from providing services under the Authorized User Agreement, they may be subject to all onboarding and security clearance requirements if they are returned to performing services under the Authorized User Agreement.

All Contractor Staff shall, at the termination of their providing services to ITS under this RFQ, comply with all State off-boarding and security procedures, including return to ITS of any physical or logical access badges or other credentials that were issued by the State and required for their access to NYS Confidential Information or Data or NYS Facilities or Data Centers.

10. ACCESS TO REGULATED DATA

The Contractor agrees to comply with the requirements listed in Appendix F for those Applicable Statutory Requirements indicated on the cover page of this RFQ. In addition to the terms found in the Contract and Appendix F, the following provisions shall apply to this RFQ.

Criminal Justice Information Services

The Contractor agrees to comply with all requirements in the most recent approved version Criminal Justice Information Services (CJIS) Security Policy, available at https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center/view and the terms of the CJIS Security Addendum below. As of the date of this RFQ, the most recent approved version of the CJIS Security Policy is Version 5.9.5, dated July 9, 2024.

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks, and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

a. Investigate or decline to investigate any report of unauthorized use.

b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer
Criminal Justice Information Services Division, FBI
1000 Custer Hollow Road
Clarksburg, West Virginia 26306

Safeguarding Federal Tax Information

I. PERFORMANCE

In performance of this Contract, the Contractor agrees to comply with and assume responsibility for compliance by Contractor Staff with the following requirements:

(1) All work will be performed under the supervision of the Contractor.

(2) The Contractor and Contractor Staff to be authorized access to Federal Tax Information (FTI) must meet the background check requirements defined in IRS Publication 1075. The Contractor will maintain a list of Contractor Staff authorized access to FTI. Such list will be provided to ITS and, upon request, to the IRS.

(3) FTI made available in any format shall be used only for the purpose of carrying out the provisions of this Contract. FTI in any format shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this Contract. Inspection by or disclosure of FTI to anyone other than the Contractor or Contractor Staff authorized is prohibited.
(4) All FTI will be accounted for upon receipt and properly stored before, during, and after processing. In addition, any related output and products will be given the same level of protection as required for the source material.
(5) The Contractor will certify that the FTI processed during the performance of this Contract will be completely purged from all physical and electronic data storage with no output to be retained by the Contractor at the time the work is completed. If immediate purging of physical and electronic data storage is not possible, the Contractor will certify that any FTI in physical or electronic storage will remain safeguarded to prevent unauthorized disclosures.
(6) Any spoilage or any intermediate hard copy printout that may result during the processing of FTI will be given to ITS. When this is not possible, the Contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts and will provide ITS with a statement containing the date of destruction, description of material destroyed, and the destruction method.
(7) All computer systems receiving, processing, storing, or transmitting FTI must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to FTI.
(8) No work involving FTI furnished under this Contract will be subcontracted without prior written approval of the IRS.
(9) Contractor will ensure that the terms of FTI safeguards described herein are included, without modification, in any approved subcontract for work involving FTI.
(10) To the extent the terms, provisions, duties, requirements, and obligations of this Contract apply to performing services with FTI, the Contractor shall assume toward the subcontractor all obligations, duties, and responsibilities that ITS under this Contract assumes toward the Contractor, and the subcontractor shall assume toward the Contractor all the same obligations, duties and responsibilities which the Contractor assumes toward ITS under this Contract.
(11) In addition to the subcontractor's obligations and duties under an approved subcontract, the terms and conditions of this Contract apply to the subcontractor, and the subcontractor is bound and obligated to the Contractor hereunder by the same terms and conditions by which the contractor is bound and obligated to ITS under this Contract.
(12) For purposes of this contract, the term "contractor" includes any officer or employee of the contractor with access to or who uses FTI, and the term "subcontractor" includes any officer or employee of the subcontractor with access to or who uses FTI.
(13) ITS will have the right to void the Contract if the Contractor fails to meet the terms of FTI safeguards described herein.

II. CRIMINAL/CIVIL SANCTIONS

(1) Each Contractor Staff of a Contractor to whom FTI is or may be disclosed shall be notified in writing that FTI disclosed to such Contractor Staff can be used only for a purpose and to the extent authorized herein, and that further disclosure of any FTI for a purpose not authorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution.
(2) Each Contractor Staff of a Contractor to whom FTI is or may be accessible shall be notified in writing that FTI accessible to such Contractor Staff may be accessed only for a purpose and to the extent authorized herein, and that access/inspection of FTI without an official need-to-know for a purpose not authorized herein constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution.
(3) Each Contractor Staff of a Contractor to whom FTI is or may be disclosed shall be notified in writing that any such unauthorized access, inspection or disclosure of FTI may also result in an award of civil damages against the Contractor Staff in an amount equal to the sum of the greater of $1,000 for each unauthorized access, inspection, or disclosure, or the sum of actual damages sustained as a result of such unauthorized access, inspection, or disclosure, plus in the case of a willful unauthorized access, inspection, or disclosure or an unauthorized access/inspection or disclosure which is the result of gross negligence, punitive damages, plus the cost of the action. These penalties are prescribed by IRC sections 7213, 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.
(4) Additionally, it is incumbent upon the Contractor to inform its Contractor Staff of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1),

which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of their employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.
(5) Granting a contractor access to FTI must be preceded by certifying that each Contractor Staff understands ITS's security policies and procedures for safeguarding FTI. The Contractor and Contractor Staff must maintain their authorization to access FTI through annual recertification of their understanding of ITS's security policy and procedures for safeguarding FTI. The initial certification and recertifications must be documented and placed in the ITS's files for review. As part of the certification and at least annually afterwards, the Contractor and each Contractor Staff must be advised of the provisions of IRC sections 7213, 7213A, and 7431 (see Exhibit 4, *Sanctions for Unauthorized Disclosure*, and Exhibit 5, *Civil Damages for Unauthorized Disclosure*). The training on ITS's security policies and procedures provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches (See Section 10). For the initial certification and the annual recertifications, the Contractor and each Contractor Staff must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. INSPECTION

The IRS and ITS, with 24-hour notice, shall have the right to send its inspectors into the offices and plants of the Contractor to inspect facilities and operations performing any work with FTI under this Contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process, or transmit FTI. Based on the inspection, corrective actions may be required in cases where the Contractor is found to be noncompliant with FTI safeguard requirements.

COMPLIANCE WITH HIPAA (HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996), HI-TECH (HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT OF 2009), AND OTHER HEALTH INFORMATION PRIVACY AND SECURITY LAWS

Definitions:
The following terms used in this Section shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information (PHI), Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

(a) Business Associate. "Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, and in this Section may refer to Contractor or its Subcontractor(s), to the extent Contractor or its Subcontractor(s) create, receive, maintain, or transmit protected health information on behalf of ITS.

(b) Covered Entity. By entering into the Contract, ITS does not affirm that it necessarily meets the definition of a "Covered Entity" or a "Business Associate" under the HIPAA statute, and rather affirms that ITS may in a given instance be acting as a "conduit" or in another capacity providing services to other entities, some of which themselves may be covered entities. But to the extent ITS is deemed to be covered by HIPAA or HI-TECH, the Parties agree the term "Covered Entity" in this Section shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103.

(c) HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

(d) "Medicaid Confidential Data" (MCD) includes all information about a Medicaid recipient or applicant, including enrollment information, eligibility data and protected health information. The NYS Department of Health (DOH) is the Single State Agency responsible for the administration of the New York State Medicaid program in New York State, including ensuring the security and confidentiality of MCD data.

HIPAA Protected Health Information Obligations and Activities of Contractor

To the extent Contractor or its Subcontractor(s) create, receive, maintain, or transmit protected health information on behalf of ITS pursuant to their responsibilities under the Contract, Contractor agrees that it is subject to, will abide by, and will require in writing its Subcontractors to similarly abide by, the following requirements applicable to Business Associates under HIPAA, agreeing to:

(a) Not use or disclose protected health information other than as permitted or required by the Contract or as required by law.

(b) Use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Contract.

(c) Report to ITS within ten (10) business days or fewer any use or disclosure of protected health information not provided for by the Contract of which it becomes aware. In no event shall Contractor exceed the timeframe for reporting to ITS breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware. Contractor shall provide ITS all information reasonably requested by ITS concerning any breach. Contractor shall also provide the following information to ITS upon first instance of the notification of breach: the identification of each individual whose unsecured protected health information has been, or is reasonably believed by Contractor, to have been, accessed, acquired, used, or disclosed during the breach.

(d) In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any Subcontractors that create, receive, maintain, or transmit protected health information on behalf of Contractor agree in writing to the same restrictions, conditions, and requirements that apply to Contractor with respect to such information.

(e) Make available protected health information in a designated record set to ITS, in a manner to be prescribed by ITS within a reasonable timeframe not to exceed fifteen (15) days, absent extenuating circumstances, as necessary to satisfy obligations which ITS or the entities it provides services to reasonably believe applicable to them under 45 CFR 164.524. In the event Contractor or its Subcontractor(s) receive any request for such protected health information directly from an individual, Contractor shall refer such request to ITS within a reasonable timeframe not to exceed ten (10) business days.

(f) Make any amendment(s) to protected health information in a designated record set as directed by ITS pursuant to 45 CFR 164.526 or take other measures as necessary to satisfy obligations that ITS reasonably believes it has under 45 CFR 164.526, in the manner as prescribed by ITS and within twenty (20) business days of such request. In the event Contractor or its Subcontractor(s) receive any request to amend a data set directly from an individual, Contractor shall refer such request to ITS within a reasonable timeframe not to exceed ten (10) business days.

(g) Maintain and make available the information required to provide an accounting of disclosures to ITS as necessary to satisfy obligations that ITS reasonably believes it has under 45 CFR 164.528, in the manner as prescribed by ITS and within ten (10) business days of such request. In the event Contractor or its Subcontractor(s) receive any request for an accounting of disclosures directly from an individual, Contractor shall refer such request to ITS within a reasonable timeframe not to exceed ten (10) business days.

(h) To the extent Contractor or its Subcontractor(s) are to carry out one or more of obligation(s) ITS may have under Subpart E of 45 CFR Part 164, in performing such obligations, comply with the requirements of Subpart E that apply to ITS; and

(i) Make either Contractor's or its Subcontractor(s)', or both's, internal practices, books, and records available to the Secretary of the Department of Health and Human Services and to ITS, for purposes of determining compliance with the HIPAA and HI-TECH Rules.

Permitted Uses and Disclosures of Protected Health Information by Contractor and its Subcontractor(s)

(a) Contractor and its Subcontractor(s) may only use or disclose protected health information as necessary to perform the services set forth in the Contract, provided however, that if de-identified information can be used in lieu of individually identifiable health information with the same effect, Contractor and its Subcontractor(s) shall use de-identified information in their performance of the Contract in accordance with 45 CFR 164.514(a)-(c).

(b) Contractor and its Subcontractor(s) may use or disclose protected health information as required by law.

(c) Contractor and its Subcontractor(s) agrees to make only those uses, disclosures and requests for protected health information that are consistent with the minimum necessary policies and procedures of ITS or the entit(ies) for whom ITS provides services which entail the creation, reception, maintenance, or transmittal of protected health information.

(d) Contractor and its Subcontractor(s) may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 except as may be provided for in the Contract or for the proper management and administration of Contractor or its Subcontractor(s), including the carrying out of the Contractor's or its Subcontractor(s)' legal responsibilities.

Other Health Information Obligations and Activities of Contractor

Contractor or its Subcontractor(s) may not disclose other types of health information protected by federal, State, or local law including but not limited to personally identifiable mental health information protected under NYS Mental Hygiene Law §33.16, other personally identifiable health information or HIV information protected under NYS Health Law sections §18 or Article 27-F, or substance abuse information protected under federal regulations 42 CFR Part 2.

Contractor or its Subcontractor(s) may not disclose Medicaid Confidential Data without the prior written approval of the New York State Department of Health (DOH), either directly or as provided to Contractor or its Subcontractor(s) through ITS. If contacted by DOH, while also informing ITS, Contractor or its Subcontractor(s) shall reasonably work with DOH to identify any individuals who may have inappropriately or unlawfully accessed Medicaid Confidential Data.

Contractor agrees to ensure that Contractor and any agent, including a Subcontractor, to whom Contractor provides Medicaid Confidential Data, agrees to the same restrictions and conditions that apply throughout the Contract. Further, Contractor agrees to state in any such agreement, contract, or document that the party to whom Contractor is providing the Medicaid Confidential Data may not further disclose it without the prior written approval of the New York State Department of Health. Contractor agrees to include the notices preceding, as well as references to statutory and regulatory citations set forth above, in any agreement, contract or document that Contractor enters into that involves Medicaid Confidential Data.

The federal Center for Medicare and Medicaid Services (CMS) requires that all contracts and/or agreements executed between the Department of Health and any second party that will receive Medicaid Confidential Data must include contract language that will bind such Parties to ensure that contractor(s) abide by the regulations and laws that govern the protection of individual, Medicaid confidential level data.

Medicaid Confidential Data includes all information about a recipient or applicant, including enrollment information, eligibility data and protected health information.

Contractor must comply with the following State and federal laws and regulations:

- Section 367b(4) of the NY Social Services Law
- New York State Social Services Law Section 369 (4)
- NYS Mental Hygiene Law §33.16,
- Article 27-F of the New York Public Health Law & 18 NYCRR 360-8.1
- Social Security Act, 42 USC 1396a (a)(7)
- Federal regulations at 42 CFR 431.302, 42 C.F.R. Part 2
- The Health Insurance Portability and Accountability act (HIPAA), at 45 CFR Parts 160 and 164

Please note that Medicaid Confidential Data released to Contractor may contain AIDS/HIV related NYS Confidential Information as defined in Section 2780(7) of the New York Public Health Law. As required by New York Public Health Law Section 2782(5), the following notice is provided to Contractor:

"This information has been disclosed to you from confidential records which are protected by state law. State law prohibits you from making any further disclosure of this information without the specific written consent of the person to whom it pertains, or as otherwise permitted by law. Any unauthorized further disclosure in violation of state law may result in a fine or jail sentence or both. A general authorization for the release of medical or other information is NOT sufficient authorization for the release for further disclosure."

Alcohol and Substance Abuse Related Confidentiality Restrictions:

Alcohol and substance abuse information is confidential pursuant to 42 C.F.R. Part 2. General authorizations are ineffective to obtain the release of such data. The federal regulations provide for a specific release for such data.

Term and Termination

(a) Termination for cause under HIPAA or HI-TECH. The Term of this Section shall be as described elsewhere in the "Term" section of the Contract. Among the other reasons for which ITS may terminate the Contract prior to the end of its Term date for cause, ITS may terminate the Contract if ITS determines the Contractor or its Subcontractor(s) have violated a material term of this HIPAA and HI-TECH Compliance Section of the Contract, and Contractor or its Subcontractor(s) have not cured the breach or ended the violation within any time that has been specified by ITS.

(b) Contractor's and its Subcontractor(s)' Obligations Upon Termination. Upon termination of the Contract for any reason, Contractor and its Subcontractor(s) shall return to ITS, transfer to another of ITS' contractors as directed by ITS, or, if agreed to by ITS on an individual case-by-case basis, destroy all protected health information received from ITS, or created, maintained, or received by the Contractor and its Subcontractor(s) on behalf of ITS, that the Contractor and its Subcontractor(s) still maintain in any form. Contractor and its Subcontractor(s) shall retain no copies of the protected health information. Contractor understands and agrees and will require of its Subcontractor(s) in writing that Contractor and its Subcontractor(s) are required to receive written approval from ITS prior to the return, transfer, or destruction of any protected health information.

(c) Survival. Contractor's and its Subcontractor(s)' obligations under this HIPAA and HI-TECH Compliance section of the Contract shall survive the termination of the Contract.

Miscellaneous

(a) Regulatory References. A reference in the Contract to a section in the HIPAA or HI-TECH Rules means the section as in effect or as amended.

(b) Amendment. The Parties agree to take such action as is necessary to amend the Contract from time to time as is necessary for compliance with the requirements of the HIPAA or HI-TECH Rules and any other applicable law.

(c) Interpretation. Any ambiguity in the Contract shall be interpreted to permit compliance with the HIPAA or HI-TECH Rules.

(d) Sub-contractors. Contractor shall require any Subcontractors that it uses that create, receive, maintain, or transmit protected health information on behalf of ITS under the Contract to conform to these HIPAA and HI-TECH Compliance requirements in addition to any other security, privacy, or applicable terms of the Contract.

D. QUESTIONS

All questions shall be emailed to the Designated Contact E-Mail Address indicated on the Cover Page of this RFQ.

Contractors are strongly encouraged to submit questions as early as possible. However, all questions must be submitted by the Question due date and time listed on the Cover Page of this RFQ. Answers to all questions of a substantive nature shall be provided to all Contractors who received this RFQ in the form of a question-and-answer document.

All Bids must conform to the terms set forth in this RFQ and the OGS Information Technology Umbrella Contract – Manufacturer Based. Extraneous terms or material deviations (including additional, inconsistent, conflicting, or alternative terms) may render the Bid non-responsive and may result in rejection of the Bid. Extraneous terms submitted on standard, pre-printed forms (including but not limited to product literature, order forms, license agreements, contracts, or other documents) that are attached or referenced with submissions shall not be considered part of the Bid or Authorized User Agreement but shall be deemed included for informational or promotional purposes only.

Each proposed extraneous term must be specifically enumerated in writing and specify the section of this RFQ that Bidder proposes to modify and the reasons why. Any extraneous terms must be submitted during the Question-and-Answer period as listed on the Cover Page of this RFQ. Extraneous terms submitted after this time will not be considered.

No extraneous term shall be incorporated into the Authorized User Agreement unless expressly accepted by ITS in writing. Acceptance and/or processing of a Bid shall not constitute acceptance of extraneous terms.

E. DOWNSTREAM PROHIBITION

None.

F. AUTHORIZED USER DISPUTE RESOLUTION PROCESS

Should a dispute or protest arise regarding this RFQ, the dispute or protest will be considered and decided by the Authorized User.

1. Disputes or Controversies Occurring During the Term of the Authorized User Agreement.
In the event there is a dispute or controversy during the term of the Authorized User Agreement resulting from this RFQ, the Contractor and Authorized User agree to exercise their best efforts to resolve the dispute as soon as possible. The Contractor and Authorized User shall, without delay, continue to perform their respective obligations under the resulting Authorized User Agreement and this Centralized Contract which are not affected by the dispute. Primary responsibility for resolving any dispute arising under the Authorized User Agreement shall rest with the persons designated by the Authorized User and the Contract's Contract Administrator and/or Account Manager.

In the event the Authorized User is dissatisfied with the Contractor's Products provided under the Authorized User Agreement, the Authorized User shall notify the Contractor in writing pursuant to the terms of the Contract. In the event the Contractor has any disputes with the Authorized User, the Contractor shall so notify the Authorized User in writing. If either party notifies the other of such dispute or controversy, the other party shall then make good faith efforts to solve the problem or settle the dispute amicably, including meeting with the party's representatives to attempt diligently to reach a satisfactory result.

If negotiation between such persons fails to resolve any such dispute to the satisfaction of the parties within fourteen (14) business days or as otherwise agreed to by the Contractor and Authorized User, of such notice, then the matter shall be submitted to the persons designated by the Authorized User and the Contractor's senior officer of the rank of Vice President or higher as its representative. Such representatives shall meet in person and shall attempt in good faith to resolve the dispute within the next fourteen (14) business days or as otherwise agreed to by the parties. This meeting must be held before either party may seek any other method of dispute resolution, including judicial or governmental resolutions. Notwithstanding the foregoing, nothing in this section shall be construed to prevent either party from seeking and obtaining temporary equitable remedies, including injunctive relief.

The Contractor shall extend the dispute resolution period for so long as the Authorized User continues to make reasonable efforts to cure the breach, except with respect to disputes about the breach of payment of fees or infringement of its or its licensors' intellectual property rights.

G. RESERVED RIGHTS

Bidders are hereby notified that New York State reserves the right to:

1. Reject any or all Bids received in response to the solicitation.
2. Withdraw the solicitation at any time, at the Agency's sole discretion.
3. Make an award under the solicitation in whole or in part.
4. Disqualify any Bidder whose conduct and/or Bid fails to conform to the requirements of the solicitation.
5. Seek clarifications and revisions of Bids.
6. Prior to the Bid deadline, amend the solicitation requirements to correct errors or oversights, or to supply additional information, as it becomes available.
7. Prior to the Bid deadline, direct Bidders to submit Bid modifications addressing subsequent solicitation amendments.
8. Change any of the schedule dates with timely notification to all prospective Bidders.
9. Eliminate any mandatory, non-material specifications that cannot be complied with by all of the prospective Bidders.
10. Waive any requirements that are not material.
11. Utilize any and all ideas submitted in the Bids received.
12. Negotiate with the Bidder responding to the solicitation within the solicitation requirements to serve the best interests of the State. This includes requesting increased discounts and clarifications of any or all Bidder's' Bids.
13. Require clarification at any time during the procurement process and/or require correction of arithmetic or other apparent errors for the purpose of assuring a full and complete understanding of a Bidder's Bid and/or to determine a Bidder's compliance with the requirements of the solicitation; and
14. Select and award to other than the selected Bidder(s) in the event of unsuccessful negotiations or, optionally, in other specified circumstances as detailed in the solicitation requirements.

15. Purchase none, some, all or more of the quantities of the items listed in Attachment 1 under this RFQ.
16. If applicable, consultants will be required to comply with ITS policies and procedures; pass background checks; and sign non-disclosure agreements.
17. If applicable, vendors may be required to complete Form A – Consultant Disclosure Form.
18. Extend the term of this agreement in accordance with the above outlined solicitation.

Manufacturer / Authorized Reseller Information

This Page is to be Completed By the Manufacturer or Authorized Reseller Responding to the RFQ

The RFQ Response must be fully and properly executed by an authorized person. By signing you certify your express authority to sign on behalf of yourself, your company, or other entity and full knowledge and acceptance of this RFQ (including any Questions/Answers or addenda), the OGS Centralized Contract and that all information provided is complete, true and accurate. Quotes received by RFQ due date/time are binding and non-retractable for 120 days or as stipulated in the RFQ.

Contract #	Manufacturer Name	Authorized Reseller Name
PM67982	Google LLC	Currier, McCabe and Associates, Inc

Manufacturer or Reseller Signature: Rachel Harpootlian *Date:* 11/4/2024	*Phone Number:* (518) 783-9003 *E-Mail:* rharpootlian@cma.com
Printed or Typed Name: Rachel Harpootlian	*Title:* CFO

If you are not providing a RFQ Response, place an "x" in the box, please explain why you are not responding, and return this page only.

☐ WE ARE UNABLE TO RESPOND AT THIS TIME BECAUSE:

After fully completing the information above, please submit this page via e-mail with "Request for Quote – Financial Response – Cloud Solution" (Excel) to the Authorized User indicated on the Cover Page. Authorized User reserves the right to request the original executed page of this RFQ.

NON-COLLUSIVE BIDDING CERTIFICATION REQUIRED BY SECTION 139-D OF THE STATE FINANCE LAW

SECTION 139-D, Statement of Non-Collusion in bids to the State:

BY SUBMISSION OF THIS BID, BIDDER AND EACH PERSON SIGNING ON BEHALF OF BIDDER CERTIFIES, AND IN THE CASE OF JOINT BID, EACH PARTY THERETO CERTIFIES AS TO ITS OWN ORGANIZATION, UNDER PENALTY OF PERJURY, THAT TO THE BEST OF HIS/HER KNOWLEDGE AND BELIEF:

[1] The prices of this bid have been arrived at independently, without collusion, consultation, communication, or agreement, for the purposes of restricting competition, as to any matter relating to such prices with any other Bidder or with any competitor;

[2] Unless otherwise required by law, the prices which have been quoted in this bid have not been knowingly disclosed by the Bidder and will not knowingly be disclosed by the Bidder prior to opening, directly or indirectly, to any other Bidder or to any competitor; and

[3] No attempt has been made or will be made by the Bidder to induce any other person, partnership or corporation to submit or not to submit a bid for the purpose of restricting competition.

A BID SHALL NOT BE CONSIDERED FOR AWARD NOR SHALL ANY AWARD BE MADE WHERE [1], [2], [3] ABOVE HAVE NOT BEEN COMPLIED WITH; PROVIDED HOWEVER, THAT IF IN ANY CASE THE BIDDER(S) CANNOT MAKE THE FOREGOING CERTIFICATION, THE BIDDER SHALL SO STATE AND SHALL FURNISH BELOW A SIGNED STATEMENT WHICH SETS FORTH IN DETAIL THE REASONS THEREFORE:

Subscribed to under penalty of perjury under the laws of the State of New York, this 4 day of November, 2024 as the act and deed of said corporation of partnership.

STATE OF NEW YORK }

} SS

COUNTY OF Albany }

On the 4th day of November in the year of 2024, before me personally appeared Rachel Hippolitan, personally known to me or proved to me on the basis of satisfactory evidence to be the individual whose name is subscribed to the foregoing Non-collusive Bidding Certification (instrument) and acknowledged to me that he/she executed the same in his/her capacity, and on his/her own behalf.

Melissa M Ellis

Notary Public

Registration No:

MELISSA M ELLIS
NOTARY PUBLIC, STATE OF NEW YORK
Registration No. 01EL6444430
Qualified in Schenectady County
Commission Expires 11/28/2026

IF BIDDER(S) (ARE) A PARTNERSHIP, COMPLETE THE FOLLOWING:

NAMES OF PARTNERS OR PRINCIPALS	LEGAL RESIDENCE

IF BIDDER(S) (ARE) A CORPORATION, COMPLETE THE FOLLOWING:

NAME	LEGAL RESIDENCE
Kenneth M. Romanski	4111 South Ocean Blvd, Highland Beach, FL 33487
President: Michele McCabe	221 Field Hill Rd, Conway, MA 01341
Secretary:	
Treasurer:	

Identifying Data

Potential Contractor Currier, McCabe and Associates, Inc. dba CMA Consulting Services

Address 700 Troy Schenectady Rd
Street
Latham, NY 12110
City, Town, etc.

Telephone (518) 783-9003 (If applicable, Responsible Corporate Officer)

Name Rachel Harpootlian Title CFO

Signature

Joint or combined bids by companies or firms must be certified on behalf of each participant.

Currier, McCabe and Associates, Inc. dba CMA Consulting Services	
Legal name of person, firm or corporation	Legal name of person, firm or corporation
By Rachel Harpootlian	
Name	Name
CFO	
Title	Title
Address 700 Troy Schenectady Rd	Address
Street	Street
Latham NY 12110	
City State	City State

Request for Quote - Financial Response - Cloud Solution

RFQ Number	Authorized User Name	Contract Number	Manufacturer / Reseller Name	Date Completed	Grand Total
ITS-2024-526DB-Google Cloud SA	Information Technology Services (ITS)	PM67982	Currier, McCabe and Associates, Inc.	11/4/2024	$55,570,267.84

Unanticipated Enhancements to Services is only applicable to items in Lot 4 - Implementation Services and is calculated based on the percentage the Authorized User chooses in cell E7 (not to exceed 20%).

Unanticipated Enhancements to Services (Not to Exceed 20%)	Implementation Base Total (*without* Unanticipated Enhancements)	Implementation Total (*with* Unanticipated Enhancements)	Recurring Cost Total	Data Transfer Cost Total
0%	$0.00	$0.00	$55,570,267.84	$0.00

Please See Request for Quotes for all Authorized User requirements.

Lot this RFQ Applies to: ☐ Lot 1 Software ☐ Lot 2 Hardware ☑ Lot 3 Cloud ☐ Lot 4 Implementation

If the RFQ includes Lot 4 – Implementation, Contractor must prior to submitting a response to the RFQ either hold an award for Lot 4- Implementation, or be able to provide the services under the other Lots included in the RFQ.

Instructions for When SKU's Have Been Identified by Authorized User

Authorized User will complete RFQ Number, Authorized User Name, Unanticipated Enhancements to Services Percent, Deliverable Number, Deliverable Name, Lot Number, Product Description(s), Manufacturer Part Number(s) (SKU), Net NYS Contract Price(s) and Qty, and Data Transfer Specifications in each of the three sections: Implementation Items, Recurring Items, and Data Transfer Items. The totals of each of these three sections will calculate into the Total Deliverable Cost. Please note, any anticipated deliverable travel costs are only applicable to items in Lot 4 - Implementation Services.
Manufacturer / Reseller will complete Deliverable Narrative, Additional Product Discount (Percentage), and optional Additional Product Discount (Dollars).

Instructions for When Authorized User Requires Vendor to Provide Suggested SKU's

Authorized User will complete RFQ Number and Authorized User Name, Unanticipated Enhancements to Services Percent, and Data Transfer Specifications in each of the three sections: Implementation Items, Recurring Items, and Data Transfer Items. The totals of each of these three sections will calculate into the Total Deliverable Cost. Please note, any anticipated deliverable travel costs are only applicable to items in Lot 4 - Implementation Services.
Manufacturer / Reseller will complete Deliverable Number, Deliverable Name, Deliverable Narrative, Lot Number, Product Description, Manufacturer Part Number (SKU), Net NYS Contract Price, Additional Product Discount (Percentage), Qty and optional Additional Product Discount (Dollars) to meet a defined need as detailed in the Authorized User Request for Quote.
RESPONSES ARE BINDING AND NON-RETRACTABLE.

Deliverable Information

Deliverable Number	Deliverable Name

Implementation Items

RFQ Item Number	Lot Number	Product Description	Manufacturer Part Number (SKU)	Net NYS Contract Price	Additional Product Discount (Percentage)	RFQ Product Price	Qty	Additional Product Discount (Dollars)	Extended RFQ Price	Unanticipated Enhancements to Services (Not to Exceed 20%)
1										
2										
3										
4										
5										
								Anticipated Deliverable Travel Costs (Lot 4 - Implementation Services only)		$0.00
								Total Deliverable Implementation Cost	$0.00	$0.00

RFQ Number	Authorized User Name	Contract Number	Manufacturer / Reseller Name	Date Completed	Grand Total
ITS-2024-526DB-Google Cloud SA	Information Technology Services (ITS)	PM67982	Currier, McCabe and Associates, Inc.	11/4/2024	$55,570,267.84

Unanticipated Enhancements to Services is only applicable to items in Lot 4 - Implementation Services and is calculated based on the percentage the Authorized User chooses in cell E7 (not to exceed 20%).

Unanticipated Enhancements to Services (Not to Exceed 20%)	Implementation Base Total (*without* Unanticipated Enhancements)	Implementation Total (*with* Unanticipated Enhancements)	Recurring Cost Total	Data Transfer Cost Total
0%	$0.00	$0.00	$55,570,267.84	$0.00

Please See Request for Quotes for all Authorized User requirements.

Recurring Items

RFQ Item Number	Lot Number	Product Description	Manufacturer Part Number (SKU)	Net NYS Contract Price	Additional Product Discount (Percentage)	RFQ Product Price	Qty	Additional Product Discount (Dollars)	Extended RFQ Price
		Year One - Term Dates to be determined							
1	Lot 3	Enterprise Agreement for Public Sector Subscription Used for a fixed price offering (not pay-as-you-go) with quantity calculated by Google up front for 1, 2, or 3 years. Prepaid with no true ups required during the 1, 2, or 3 year period covered by the fixed price. Includes unlimited Google Cloud access, but is not an aggregate of skus, and not on a per seat license basis. No professional services included. Not maintenance or support of other Google Cloud Products. Not a customer-specific sku but instead available to all public sector customers (listed on Google's Manufacturer's Price List with a list Price).	9A92-40AE-8D00	$0.99			8728507.00		$8,641,221.93
2	Lot 3	GCP Points-Access to all GCP Solutions-Compute, Storage & Databases, Networking, Big Data Data Transfer, Machine Learning, APIs, IoT, Management, Developer and Security Tools- Payment-Monthly based Usage	G-POINTS-MON	$0.99			5588297.00		$5,532,414.03
3	Lot 3	Bytes of data ingested in US for the Enterprise Plus package under subscription	70CB-8A2E-163E	$4.51			800000.00		$3,608,000.00
4	Lot 3	Monthly BeyondCorp Enterprise Users (Month) Qty 114,000 times 12 months = 1,368,000	E2D2-474B-B4EF	$5.88			1368000.00		$8,043,840.00
5	Lot 3	Platform Elite - Customer Hosted - Looker by Google Qty 5 times 12 months = 60	Looker-105	$14,700.00			60.00		$882,000.00
6	Lot 3	GCP Support Base - Region 1 countries Qty 4 times 12 months = 48	SUPPORT-GCP-BASE-PREM-REG1	$12,250.00			48.00		$588,000.00
		Year Two- Term Dates to be determined							$0.00
7	Lot 3	Enterprise Agreement for Public Sector Subscription Used for a fixed price offering (not pay-as-you-go) with quantity calculated by Google up front for 1, 2, or 3 years. Prepaid with no true ups required during the 1, 2, or 3 year period covered by the fixed price. Includes unlimited Google Cloud access, but is not an aggregate of skus, and not on a per seat license basis. No professional services included. Not maintenance or support of other Google Cloud Products. Not a customer-specific sku but instead available to all public sector customers (listed on Google's Manufacturer's Price List with a list Price).	9A92-40AE-8D00	$0.99			9322032.00		$9,228,811.68
8	Lot 3	GCP Points-Access to all GCP Solutions-Compute, Storage & Databases, Networking, Big Data Data Transfer, Machine Learning, APIs, IoT, Management, Developer and Security Tools- Payment-Monthly based Usage	G-POINTS-MON	$0.99			5983980.00		$5,924,140.20
9	Lot 3	Bytes of data ingested in US for the Enterprise Plus package under subscription	70CB-8A2E-163E	$4.51			800000.00		$3,608,000.00
10	Lot 3	Monthly BeyondCorp Enterprise Users (Month) Qty 114,000 times 12 months = 1,368,000	E2D2-474B-B4EF	$5.88			1368000.00		$8,043,840.00
11	Lot 3	Platform Elite - Customer Hosted - Looker by Google Qty 5 times 12 months = 60	Looker-105	$14,700.00			60.00		$882,000.00
12	Lot 3	GCP Support Base - Region 1 countries Qty 4 times 12 months = 48	SUPPORT-GCP-BASE-PREM-REG1	$12,250.00			48.00		$588,000.00
13									
14									
15									
								Total Deliverable Recurring Cost	$55,570,267.84

RFQ Number	Authorized User Name	Contract Number	Manufacturer / Reseller Name	Date Completed	Grand Total
ITS-2024-526DB-Google Cloud SA	Information Technology Services (ITS)	PM67982	Currier, McCabe and Associates, Inc.	11/4/2024	$55,570,267.84

Unanticipated Enhancements to Services is only applicable to items in Lot 4 - Implementation Services and is calculated based on the percentage the Authorized User chooses in cell E7 (not to exceed 20%).

Unanticipated Enhancements to Services (Not to Exceed 20%)	Implementation Base Total (*without* Unanticipated Enhancements)	Implementation Total (*with* Unanticipated Enhancements)	Recurring Cost Total	Data Transfer Cost Total
0%	$0.00	$0.00	$55,570,267.84	$0.00

Please See Request for Quotes for all Authorized User requirements.

Data Transfer Items

Data Transfer Specifications:

RFQ Item Number	Lot Number	Product Description	Manufacturer Part Number (SKU)	Net NYS Contract Price	Additional Product Discount (Percentage)	RFQ Product Price	Qty	Additional Product Discount (Dollars)	Extended RFQ Price	Unanticipated Enhancements to Services (Not to Exceed 20%)
1										
2										
3										
4										
5										
								Anticipated Deliverable Travel Costs (Lot 4 - Implementation Services only)		
								Total Deliverable Data Transfer Cost	$0.00	$0.00

Total Deliverable Cost	$55,570,267.84

Cover Page – Request for Quote – Cloud Solution

TO BE COMPLETED BY AUTHORIZED USER

RFQ Title **Google Cloud SA** **RFQ Number** ITS-2024-526DB

Authorized User Information:
Office of Information Technology Services
Empire State Plaza
Swan Street Building, Core 4
2nd Floor, Room 2404
Albany, NY 12223

Authorized User Delivery Information:
Joseph Marshall
NYS Office of Information Technology Services
Swan Street Bldg, Core 4, Floor 3
Empire State Plaza
Albany, NY 12227

Special Delivery Instructions:

DESIGNATED CONTACTS

Name(s)	E-Mail(s)
Dominic Brefo – Contract Manager	Its.sm.ITS_BIDS@its.ny.gov

Authorized User shall indicate if Procurement Lobbying Law/Restricted Period is in effect: ☒ **Yes** ☐ **No**
Where Procurement Lobbying Law is deemed applicable by the Authorized User, by signing, Contractor affirms that it understands and agrees to comply with the Authorized User's policies and procedures relative to permissible contacts. Information may be accessed at: Procurement Lobbying:
http://www.ogs.ny.gov/aboutOgs/regulations/defaultAdvisoryCouncil.html)

RFQ LOTS

This RFQ is for Products from the following checked Lots as defined in Award # 22802 – Information Technology Umbrella Contract – Manufacturer Based (Statewide):

☐ Lot 1 – Software ☐ Lot 2 – Hardware ☒ Lot 3 - Cloud ☐ Lot 4 – Implementation

The Authorized User named above is seeking competitive quotes from the Contractor (Manufacturer) and their Resellers (where applicable) of Information Technology Umbrella Contract – Manufacturer Based Contract(s) for the above-referenced Products. If the RFQ includes Lot 4 – Implementation, Contractor must prior to submitting a response to the RFQ either hold an award for Lot 4- Implementation or be able to provide the services under the other Lots included in the RFQ.

LOT 3 – CLOUD DATA RISK LEVEL: ☐ Low ☒ Medium ☐ High

DATA CATEGORIZATION ELEMENTS: Data is all public information.

QUESTIONS AND OTHER EVENTS

Event	Date	Time
RFQ Release Date	11/1/2024	N/A
Questions Due	11/4/2024	3:00 PM EST
Vendor Response Due Date	11/5/2024	3:00 PM EST

IS THE RFQ BIDDER POOL LIMITED TO M/WBE, SB, AND SDVOB VENDORS: ☐ Yes ☒ No

BASIS FOR AWARD
☒ Lowest Price Meeting Specified Technical Requirements
☐ Lowest Price Meeting Specified Technical Requirements **and** Mandatory Pass/Fail Requirements
☐ Best Value with Technical and Financial Score

E-RATE ELIGIBLE ☐ Yes (E-Rate Discounts are Required) ☒ No

SERVICE MODEL FOR LOT 3 – CLOUD SOLUTION *(check all that apply)*
☒ Software as a Service (SaaS)
☒ Platform as a Service (PaaS)
☒ Infrastructure as a Service(IaaS)
☐ Anything as a Service (XaaS)

DEPLOYMENT MODEL FOR LOT 3 – CLOUD SOLUTION (*Check all that apply*)	☐ Private Cloud ☐ Community Cloud ☒ Public Cloud ☐ Hybrid Cloud ☐ Other
APPLICABLE STATUTORY / POLICY REQUIRMENT	☐ None ☒ CJIS ☐ FERPA ☒ FISMA ☒ GLB ☐ HIPAA ☐ HITECH ☐ Tax ☐ PPI ☐ PCI DSS ☐ SOX ☐ ECPA ☐ Other
CAIQ REQUIRMENT	☐ Yes ☒ No
ATTACHMENTS	Attachment 1 - Request for Quote – Financial Response – Cloud Solution Attachment 2 – Non-Collusive Bidding Certification Exhibit 1 – Google Master Terms and G Suite Service Schedule

The Authorized User will not be held liable for any cost incurred by the Contractor for work performed in the preparation of a response to this RFQ or for any work performed prior to the formal execution of an Authorized User Agreement. Responses to the RFQ must be received by the deadline specified above. Contractors assume all risks for timely, properly submitted deliveries. A Contractor is strongly encouraged to arrange for delivery of RFQ responses prior to the date of the RFQ opening. LATE RFQ responses may be rejected. The received time of a RFQ response will be determined by the Authorized User.

All purchases resulting from this RFQ shall be in accordance with terms and conditions of the OGS Information Technology Umbrella Contract – Manufacturer Based Contract and any additional terms and conditions set forth in this RFQ and its Attachments.

A. SCOPE / MANDATORY REQUIREMENTS

This RFQ is being distributed to the Contractor and Resellers (where applicable) to acquire the following:

1. SCOPE

This RFQ is seeking to acquire Google cloud data acquisition, compute, cybersecurity, and support products off Office of General Services centralized Google contract PM67982. These products will be used to provide centralized IT consolidation of agency contracts, satisfy existing agency demand and result in significant savings to the state thru centralization.

The term of this agreement is two years with the option to renew based upon mutual consent. Annual purchase orders will be issued. Payment of invoices will be made for actual usage on a monthly basis.

For the duration of an Authorized User Agreement, the Cloud Solution shall conform to the Cloud Solution Manufacturer's specifications, Documentation, performance standards (including applicable license terms, warranties, guarantees, Service Level Agreements, service commitments, and credits).

2. CLOUD SERVICE MODEL

Software as a Service (SaaS)
Infrastructure as a Service (IaaS)
Platform as a Service (PaaS)

3. CLOUD DEPLOYMENT MODEL

Public Cloud (Google Cloud Platform).

4. DATA CATEGORIZATION

Risk Level: Medium. All data is public information.

5. DATA OWNERSHIP

The Authorized User shall own all right, title and interest in Data.

6. DATA LOCATION

All Data shall remain in CONUS.

7. ENCRYPTION

Contractor shall use appropriate means to preserve and protect State Data. This includes, but is not limited to, use of stable storage Media, regular data backups and archiving, password protection of volumes, and data encryption. Encryption at rest as well as Encryption in flight within the Google Cloud infrastructure. Availability to leverage CMEK (Customer Managed Encryption Keys). All Data transmitted between ITS and the Contractor must comply with NYS ITS Standard NYS-S14-007 Encryption Standard (http://its.ny.gov/document/encryption-standard).

8. SECURITY

The Contractor and its personnel shall adhere to all required compliance domains, State security policies, procedures, and directives currently existing or implemented during the term of the Contract. These compliance domains and security policies include, but are not limited to, the following New York State Information Security Policies and Standards, National Institute of Standards and Technology (NIST) Policies (or their successor policies), and statutes:

P03-002 - Information Security Policy
P08-001 - Enterprise Plan to Procure Policy
P08-005 - Accessibility of Web-Based Information and Application
S13-002 - Information Classification Standard
S13-003 - Sanitation/Secure Disposal
S13-005 - Cyber Incident Response Standard
S14-002 - Information Classification Standard
S14-003 - Information Security Controls
S14-006 - Authentication Tokens Standard
S14-007 - NYS Encryption Standard

S14-010 - Remote Access
NIST Federal Information Processing Standard (FIPS) Publication 140-2
NIST Federal Information Processing Standards (FIPS) Publication 199 – Standards for Security Categorization of Federal Information and Information Systems
NIST Special Publication 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations.
NIST Special Publication 800-57, Part 1 - Recommendation for Key Management – Part 1: General
NIST Special Publication 800-088r1 - Guidelines for Media Sanitization
NIST Special Publication 800-111 - Guide to Storage Encryption Technologies for End User Devices
NIST Special Publication 800-122 - Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
NIST Special Publication 800-131A - Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths
New York State Information Security Controls Standard
New York State Risk Management Standard
Health Insurance Portability and Accountability Act of 1996

Requires implementation of Assured Workloads to meet FedRAMP Moderate compliance requirements.

CAIQ Requirement/Contractor Security:

- A Consensus Assessment Initiative Questionnaire (CAIQ) is required to be submitted by the Contractor.
- NYS ITS is retaining the right to request the CAIQ be completed annually.
- A written description of Contractor's physical/virtual security and/or internal control processes are required.
- Security Logs and Reports will need to be provided in a format communicated by NYS ITS.
- At the sole discretion of ITS, ITS may accept other audited reports in lieu of the CAIQ, provided the report meets all other requirements in this section.

The contractor warrants, covenants, and represents that it shall comply fully with all applicable ITS Information Security policies and procedures located at https://its.ny.gov/eiso/policies/security during the performance of the resulting Contract. The State may terminate the Contract if it determines that Contractor has violated a material term of this section. The terms of this section shall apply equally to Contractor, officers, agents, employees, and Subcontractors, if any. Contractor agrees that all officers, agents, employees, and Subcontractors, if any, shall be made aware of and shall agree to the terms of this section.

9. MAINTENANCE/SUPPORT

Vendor shall provide maintenance and support based on its usual commercial processes.

10. INFRASTRUCTURE SUPPORT SERVICES

Infrastructure support services that do not directly or indirectly access Data may be provided in a Follow the Sun format.

11. BUSINESS CONTINUITY/DISASTER RECOVERY (BC/DR) OPERATIONS

The Contractor must provide proof of their redundant 24x7 model including site load balancing and disaster recovery. Redundancy should span at least two highly available, secure data centers in the continental United States with a minimum of 500 miles of geographic separation. Minimum availability criteria include power supply, redundant Internet connectivity with multiple providers, fire protection, etc. Maintain full off-site back-up of operating systems, software, configurations, and any data needed to successfully recover from any hardware, software, or site failure. Disaster recovery must be tested annually.

12. AUTHENTICATION TOKENS

Authentication Tokens are required and must meet the AAL1 standard as a minimum.

13. APPLICATION PROGRAM INTERFACE (API) OR SELF ELECTRONIC PORTAL

New York State requires access to both an API and electronic portal for the purposes of accessing, downloading, and/or interacting with data within the system.

B. STATEMENT OF WORK

This is an enterprise agreement subscription and as such there is no statement of work for the contractor.

1. IMPLEMENTATION OF CLOUD SOLUTION

N/A

2. RECURRING SERVICES

The items listed in the Attachment 1.

3. TRANSFER OF DATA

N/A

Contractor cannot charge for the transfer of Data unless the charges are provided for in response to this RFQ.

C. AUTHORIZED USER TERMS AND CONDITIONS

1. DATA BREACH – REQUIRED CONTRACTOR ACTIONS

Unless otherwise provided by law, in the event of a Data Breach, the Contractor shall:
1. Notify the ITS and any potentially affected Authorized User(s), or their designated contact person(s), by telephone as soon as possible, but in no event more than 12 hours from the time the Contractor confirms the Data Breach.
2. Consult with and receive authorization from the Authorized User as to the content of any notice to affected parties prior to notifying any affected parties to whom notice of the Data Breach is required, either by statute or by the Authorized User.
3. Coordinate all communication regarding the Data Breach with the ITS and Authorized User (including possible communications with third parties).
4. Cooperate with the Authorized User, ITS and any Contractor working on behalf of the Authorized User or ITS in attempting (a) to determine the scope and cause of the breach; and (b) to prevent the future recurrence of such security breaches; and
5. Take such corrective actions that the Contractor deems necessary to contain the Data Breach. Contractor shall provide Written notice to the Authorized User as to all such corrective actions taken by the Contractor to remedy the Data Breach. Unless otherwise agreed to in the Authorized User Agreement, if Contractor is unable to complete the corrective action within the required timeframe, the remedies provided in Appendix B, Section 52, Remedies for Breach shall apply and (i) the Authorized User may contract with a third party to provide the required services until corrective actions and services resume in a manner acceptable to the Authorized User, or until the Authorized User has completed a new procurement for a replacement service system; (ii) and the Contractor will be responsible for the reasonable cost of these services during this period.

Nothing herein shall in any way (a) impair the Authorized User or OAG to bring an action against Contractor to enforce the provisions of the New York State Information Security Breach Notification Act (ISBNA) or (b) limit Contractor's liability for any violations of the ISBNA or any other applicable statutes, rules, or regulations.

2. AUTHORIZED USER ACCESS TO DATA

The Authorized User shall have access to its Data at all times, through the term of the Authorized User Agreement.

The Authorized User shall have the ability to import or export Data in piecemeal or in its entirety at the Authorized User's discretion at no charge to the Authorized User. This includes the ability for the Authorized User to import or export Data to/from other Contractors.

3. CONTRACTOR ACCESS TO DATA

The Contractor shall not copy or transfer Data unless authorized in writing by the Authorized User. In such an event the Data shall be copied and/or transferred in accordance with the provisions of this Section. Contractor shall not access any Data for any purpose other than fulfilling the service. Contractor is prohibited from Data Mining, cross tabulating, monitoring Authorized User's Data usage and/or access, or performing any other Data analytics other than those required within the Authorized User Agreement. At no time shall any Data or processes (e.g. workflow, applications, etc.), which either are owned or used by the Authorized User be copied, disclosed, or retained by the Contractor or any party related to the Contractor. Contractors are allowed to perform industry standard back-ups of Data. Documentation of back-up must be provided to the Authorized User upon request. Contractor must comply with any and all security requirements within the Authorized User Agreement.

4. SUSPENSION OF SERVICES

During any period of suspension of service, the Authorized User shall have full access to all Data at no charge. The Contractor shall not take any action to erase and/or withhold any Authorized User Data, except as directed by the Authorized User.

5. EXPIRATION OR TERMINATION OF SERVICES

Upon expiration or termination of an Authorized User Agreement, the Authorized User shall have full access to all Data for a period of 60 calendar days. During this period, the Contractor shall not take any action to erase and/or withhold any Data, except as directed by the Authorized User. An Authorized User shall have the right to specify a period more than 60 calendar days in its RFQ. There will be no additional charge to the State for this access.

6. ACCESS TO SECURITY LOGS AND REPORTS

Upon request, the Contractor shall provide access to security logs and reports to the State or Authorized User in a format as specified by the Authorized User.

7. CONTRACTOR PERFORMANCE AUDIT

The Contractor shall allow the Authorized User to assess Contractor's performance by providing any materials requested in the Authorized User including but not limited to page load times, response times, uptime, and fail over time. The Authorized User may perform this Contractor performance audit with a third party at its discretion, at the Authorized User's expense.

The Contractor shall perform an independent audit of its Data Centers, at least annually, at Contractor expense. The Contractor will provide a data owner facing audit report upon request by the Authorized User. The Contractor shall identify any confidential, trade secret, or proprietary information in accordance with Appendix B, Section 9(a), Confidential/Trade Secret Materials.

Except as otherwise provided for, all status reports and other documents produced for the State become the property of the State.

8. MODIFICATION TO CLOUD SERVICE DEPLOYMENT MODEL, SERVICE MODEL, AND/OR INITIAL FUNCTIONALITY WITHIN AN AUTHORIZED USER AGREEMENT

As Cloud services, can be flexible and dynamic, delivery mechanisms may be subject to change. This may result in changes to the deployment model, service model, functionality, or SKU. The OGS and Authorized Users require notification of any such changes to ensure security and business needs are met.

Any changes to the deployment model, service model, functionality, or SKU (e.g., PaaS to IaaS) must be provided to OGS via Appendix C - Contract Modification Procedures.

In addition, notification must be provided to the Authorized User for review and acceptance, prior to implementation. Any changes to the Authorized User Agreement will require the Authorized User to re-assess the risk mitigation methodologies and strategies and revise the Authorized User Agreement as needed.

9. BACKGROUND CHECK REQUIREMENTS

All Contractor Staff shall, prior to the commencement of any services pursuant to this RFQ, whether on or off-site, comply with all State onboarding and security clearance requirements, including training and signing certifications or agreements, required for access to NYS Confidential Information or Data or required for access to NYS Facilities or Data Centers, the preceding described, collectively, as "onboarding." This includes requirements related to the access to Regulated data, including any requirements of the State's public safety agencies, or those related to the Federal Bureau of Investigation Criminal Justice Information Services (CJIS) Security Policy (https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center).

Contractor agrees that its Contractor Staff performing services on-site at NYS Facilities or Data Centers or those with logical access to NYS Confidential Information or Data (i.e., log-in access) shall be required to undergo the same security clearances as those required of ITS employees. If not physically or virtually escorted, each Contractor Staff designated to work under the Authorized User Agreement with ITS shall submit identifying information to the State and be fingerprinted. ITS shall arrange for the scheduling of fingerprinting. Such fingerprints shall be submitted to the NYS Division of Criminal Justice Services for a state criminal history record check and, at ITS' discretion, to the Federal Bureau of Investigation for a national criminal history record check.

Contractor also agrees that its Contractor Staff performing services on-site at NYS Facilities or Data Centers may be required to comply with those health checks which NYS requires of its own employees working on-site including for example providing proof of vaccination against, and/or testing for, infectious disease such as COVID-19.

All expenses, including travel and lodging, associated with the onboarding and security clearance process including fingerprinting of Contractor Staff are the responsibility of the Contractor and are not reimbursable.

ITS shall make all suitability determinations on Contractor Staff. For purposes of this Section, a "suitability determination" is a determination that there are reasonable grounds to believe that an individual will likely be able to perform the Authorized User Agreement requirements without undue risk to the interests of the State. Failure of a security clearance or non-compliance with this Section will disqualify any Contractor Staff from performing any services on the Authorized User Agreement. If any Contractor Staff are removed from providing services under the Authorized User Agreement, they may be subject to all onboarding and security clearance requirements if they are returned to performing services under the Authorized User Agreement.

All Contractor Staff shall, at the termination of their providing services to ITS under this RFQ, comply with all State off-boarding and security procedures, including return to ITS of any physical or logical access badges or other credentials that were issued by the State and required for their access to NYS Confidential Information or Data or NYS Facilities or Data Centers.

10. ACCESS TO REGULATED DATA

The Contractor agrees to comply with the requirements listed in Appendix F for those Applicable Statutory Requirements indicated on the cover page of this RFQ. In addition to the terms found in the Contract and Appendix F, the following provisions shall apply to this RFQ.

Criminal Justice Information Services

The Contractor agrees to comply with all requirements in the most recent approved version Criminal Justice Information Services (CJIS) Security Policy, available at https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center/view and the terms of the CJIS Security Addendum below. As of the date of this RFQ, the most recent approved version of the CJIS Security Policy is Version 5.9.5, dated July 9, 2024.

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks, and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

a. Investigate or decline to investigate any report of unauthorized use.

b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer
Criminal Justice Information Services Division, FBI
1000 Custer Hollow Road
Clarksburg, West Virginia 26306

Safeguarding Federal Tax Information

I. PERFORMANCE

In performance of this Contract, the Contractor agrees to comply with and assume responsibility for compliance by Contractor Staff with the following requirements:

(1) All work will be performed under the supervision of the Contractor.

(2) The Contractor and Contractor Staff to be authorized access to Federal Tax Information (FTI) must meet the background check requirements defined in IRS Publication 1075. The Contractor will maintain a list of Contractor Staff authorized access to FTI. Such list will be provided to ITS and, upon request, to the IRS.

(3) FTI made available in any format shall be used only for the purpose of carrying out the provisions of this Contract. FTI in any format shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this Contract. Inspection by or disclosure of FTI to anyone other than the Contractor or Contractor Staff authorized is prohibited.
(4) All FTI will be accounted for upon receipt and properly stored before, during, and after processing. In addition, any related output and products will be given the same level of protection as required for the source material.
(5) The Contractor will certify that the FTI processed during the performance of this Contract will be completely purged from all physical and electronic data storage with no output to be retained by the Contractor at the time the work is completed. If immediate purging of physical and electronic data storage is not possible, the Contractor will certify that any FTI in physical or electronic storage will remain safeguarded to prevent unauthorized disclosures.
(6) Any spoilage or any intermediate hard copy printout that may result during the processing of FTI will be given to ITS. When this is not possible, the Contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts and will provide ITS with a statement containing the date of destruction, description of material destroyed, and the destruction method.
(7) All computer systems receiving, processing, storing, or transmitting FTI must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to FTI.
(8) No work involving FTI furnished under this Contract will be subcontracted without prior written approval of the IRS.
(9) Contractor will ensure that the terms of FTI safeguards described herein are included, without modification, in any approved subcontract for work involving FTI.
(10) To the extent the terms, provisions, duties, requirements, and obligations of this Contract apply to performing services with FTI, the Contractor shall assume toward the subcontractor all obligations, duties, and responsibilities that ITS under this Contract assumes toward the Contractor, and the subcontractor shall assume toward the Contractor all the same obligations, duties and responsibilities which the Contractor assumes toward ITS under this Contract.
(11) In addition to the subcontractor's obligations and duties under an approved subcontract, the terms and conditions of this Contract apply to the subcontractor, and the subcontractor is bound and obligated to the Contractor hereunder by the same terms and conditions by which the contractor is bound and obligated to ITS under this Contract.
(12) For purposes of this contract, the term "contractor" includes any officer or employee of the contractor with access to or who uses FTI, and the term "subcontractor" includes any officer or employee of the subcontractor with access to or who uses FTI.
(13) ITS will have the right to void the Contract if the Contractor fails to meet the terms of FTI safeguards described herein.

II. CRIMINAL/CIVIL SANCTIONS

(1) Each Contractor Staff of a Contractor to whom FTI is or may be disclosed shall be notified in writing that FTI disclosed to such Contractor Staff can be used only for a purpose and to the extent authorized herein, and that further disclosure of any FTI for a purpose not authorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution.
(2) Each Contractor Staff of a Contractor to whom FTI is or may be accessible shall be notified in writing that FTI accessible to such Contractor Staff may be accessed only for a purpose and to the extent authorized herein, and that access/inspection of FTI without an official need-to-know for a purpose not authorized herein constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution.
(3) Each Contractor Staff of a Contractor to whom FTI is or may be disclosed shall be notified in writing that any such unauthorized access, inspection or disclosure of FTI may also result in an award of civil damages against the Contractor Staff in an amount equal to the sum of the greater of $1,000 for each unauthorized access, inspection, or disclosure, or the sum of actual damages sustained as a result of such unauthorized access, inspection, or disclosure, plus in the case of a willful unauthorized access, inspection, or disclosure or an unauthorized access/inspection or disclosure which is the result of gross negligence, punitive damages, plus the cost of the action. These penalties are prescribed by IRC sections 7213, 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.
(4) Additionally, it is incumbent upon the Contractor to inform its Contractor Staff of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1),

which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of their employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.
(5) Granting a contractor access to FTI must be preceded by certifying that each Contractor Staff understands ITS's security policies and procedures for safeguarding FTI. The Contractor and Contractor Staff must maintain their authorization to access FTI through annual recertification of their understanding of ITS's security policy and procedures for safeguarding FTI. The initial certification and recertifications must be documented and placed in the ITS's files for review. As part of the certification and at least annually afterwards, the Contractor and each Contractor Staff must be advised of the provisions of IRC sections 7213, 7213A, and 7431 (see Exhibit 4, *Sanctions for Unauthorized Disclosure*, and Exhibit 5, *Civil Damages for Unauthorized Disclosure*). The training on ITS's security policies and procedures provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches (See Section 10). For the initial certification and the annual recertifications, the Contractor and each Contractor Staff must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. INSPECTION

The IRS and ITS, with 24-hour notice, shall have the right to send its inspectors into the offices and plants of the Contractor to inspect facilities and operations performing any work with FTI under this Contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process, or transmit FTI. Based on the inspection, corrective actions may be required in cases where the Contractor is found to be noncompliant with FTI safeguard requirements.

COMPLIANCE WITH HIPAA (HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996), HI-TECH (HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT OF 2009), AND OTHER HEALTH INFORMATION PRIVACY AND SECURITY LAWS

Definitions:
The following terms used in this Section shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information (PHI), Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

(a) Business Associate. "Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, and in this Section may refer to Contractor or its Subcontractor(s), to the extent Contractor or its Subcontractor(s) create, receive, maintain, or transmit protected health information on behalf of ITS.

(b) Covered Entity. By entering into the Contract, ITS does not affirm that it necessarily meets the definition of a "Covered Entity" or a "Business Associate" under the HIPAA statute, and rather affirms that ITS may in a given instance be acting as a "conduit" or in another capacity providing services to other entities, some of which themselves may be covered entities. But to the extent ITS is deemed to be covered by HIPAA or HI-TECH, the Parties agree the term "Covered Entity" in this Section shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103.

(c) HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

(d) "Medicaid Confidential Data" (MCD) includes all information about a Medicaid recipient or applicant, including enrollment information, eligibility data and protected health information. The NYS Department of Health (DOH) is the Single State Agency responsible for the administration of the New York State Medicaid program in New York State, including ensuring the security and confidentiality of MCD data.

HIPAA Protected Health Information Obligations and Activities of Contractor

To the extent Contractor or its Subcontractor(s) create, receive, maintain, or transmit protected health information on behalf of ITS pursuant to their responsibilities under the Contract, Contractor agrees that it is subject to, will abide by, and will require in writing its Subcontractors to similarly abide by, the following requirements applicable to Business Associates under HIPAA, agreeing to:

(a) Not use or disclose protected health information other than as permitted or required by the Contract or as required by law.

(b) Use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Contract.

(c) Report to ITS within ten (10) business days or fewer any use or disclosure of protected health information not provided for by the Contract of which it becomes aware. In no event shall Contractor exceed the timeframe for reporting to ITS breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware. Contractor shall provide ITS all information reasonably requested by ITS concerning any breach. Contractor shall also provide the following information to ITS upon first instance of the notification of breach: the identification of each individual whose unsecured protected health information has been, or is reasonably believed by Contractor, to have been, accessed, acquired, used, or disclosed during the breach.

(d) In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any Subcontractors that create, receive, maintain, or transmit protected health information on behalf of Contractor agree in writing to the same restrictions, conditions, and requirements that apply to Contractor with respect to such information.

(e) Make available protected health information in a designated record set to ITS, in a manner to be prescribed by ITS within a reasonable timeframe not to exceed fifteen (15) days, absent extenuating circumstances, as necessary to satisfy obligations which ITS or the entities it provides services to reasonably believe applicable to them under 45 CFR 164.524. In the event Contractor or its Subcontractor(s) receive any request for such protected health information directly from an individual, Contractor shall refer such request to ITS within a reasonable timeframe not to exceed ten (10) business days.

(f) Make any amendment(s) to protected health information in a designated record set as directed by ITS pursuant to 45 CFR 164.526 or take other measures as necessary to satisfy obligations that ITS reasonably believes it has under 45 CFR 164.526, in the manner as prescribed by ITS and within twenty (20) business days of such request. In the event Contractor or its Subcontractor(s) receive any request to amend a data set directly from an individual, Contractor shall refer such request to ITS within a reasonable timeframe not to exceed ten (10) business days.

(g) Maintain and make available the information required to provide an accounting of disclosures to ITS as necessary to satisfy obligations that ITS reasonably believes it has under 45 CFR 164.528, in the manner as prescribed by ITS and within ten (10) business days of such request. In the event Contractor or its Subcontractor(s) receive any request for an accounting of disclosures directly from an individual, Contractor shall refer such request to ITS within a reasonable timeframe not to exceed ten (10) business days.

(h) To the extent Contractor or its Subcontractor(s) are to carry out one or more of obligation(s) ITS may have under Subpart E of 45 CFR Part 164, in performing such obligations, comply with the requirements of Subpart E that apply to ITS; and

(i) Make either Contractor's or its Subcontractor(s)', or both's, internal practices, books, and records available to the Secretary of the Department of Health and Human Services and to ITS, for purposes of determining compliance with the HIPAA and HI-TECH Rules.

Permitted Uses and Disclosures of Protected Health Information by Contractor and its Subcontractor(s)

(a) Contractor and its Subcontractor(s) may only use or disclose protected health information as necessary to perform the services set forth in the Contract, provided however, that if de-identified information can be used in lieu of individually identifiable health information with the same effect, Contractor and its Subcontractor(s) shall use de-identified information in their performance of the Contract in accordance with 45 CFR 164.514(a)-(c).

(b) Contractor and its Subcontractor(s) may use or disclose protected health information as required by law.

(c) Contractor and its Subcontractor(s) agrees to make only those uses, disclosures and requests for protected health information that are consistent with the minimum necessary policies and procedures of ITS or the entit(ies) for whom ITS provides services which entail the creation, reception, maintenance, or transmittal of protected health information.

(d) Contractor and its Subcontractor(s) may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 except as may be provided for in the Contract or for the proper management and administration of Contractor or its Subcontractor(s), including the carrying out of the Contractor's or its Subcontractor(s)' legal responsibilities.

Other Health Information Obligations and Activities of Contractor

Contractor or its Subcontractor(s) may not disclose other types of health information protected by federal, State, or local law including but not limited to personally identifiable mental health information protected under NYS Mental Hygiene Law §33.16, other personally identifiable health information or HIV information protected under NYS Health Law sections §18 or Article 27-F, or substance abuse information protected under federal regulations 42 CFR Part 2.

Contractor or its Subcontractor(s) may not disclose Medicaid Confidential Data without the prior written approval of the New York State Department of Health (DOH), either directly or as provided to Contractor or its Subcontractor(s) through ITS. If contacted by DOH, while also informing ITS, Contractor or its Subcontractor(s) shall reasonably work with DOH to identify any individuals who may have inappropriately or unlawfully accessed Medicaid Confidential Data.

Contractor agrees to ensure that Contractor and any agent, including a Subcontractor, to whom Contractor provides Medicaid Confidential Data, agrees to the same restrictions and conditions that apply throughout the Contract. Further, Contractor agrees to state in any such agreement, contract, or document that the party to whom Contractor is providing the Medicaid Confidential Data may not further disclose it without the prior written approval of the New York State Department of Health. Contractor agrees to include the notices preceding, as well as references to statutory and regulatory citations set forth above, in any agreement, contract or document that Contractor enters into that involves Medicaid Confidential Data.

The federal Center for Medicare and Medicaid Services (CMS) requires that all contracts and/or agreements executed between the Department of Health and any second party that will receive Medicaid Confidential Data must include contract language that will bind such Parties to ensure that contractor(s) abide by the regulations and laws that govern the protection of individual, Medicaid confidential level data.

Medicaid Confidential Data includes all information about a recipient or applicant, including enrollment information, eligibility data and protected health information.

Contractor must comply with the following State and federal laws and regulations:

- Section 367b(4) of the NY Social Services Law
- New York State Social Services Law Section 369 (4)
- NYS Mental Hygiene Law §33.16,
- Article 27-F of the New York Public Health Law & 18 NYCRR 360-8.1
- Social Security Act, 42 USC 1396a (a)(7)
- Federal regulations at 42 CFR 431.302, 42 C.F.R. Part 2
- The Health Insurance Portability and Accountability act (HIPAA), at 45 CFR Parts 160 and 164

Please note that Medicaid Confidential Data released to Contractor may contain AIDS/HIV related NYS Confidential Information as defined in Section 2780(7) of the New York Public Health Law. As required by New York Public Health Law Section 2782(5), the following notice is provided to Contractor:

"This information has been disclosed to you from confidential records which are protected by state law. State law prohibits you from making any further disclosure of this information without the specific written consent of the person to whom it pertains, or as otherwise permitted by law. Any unauthorized further disclosure in violation of state law may result in a fine or jail sentence or both. A general authorization for the release of medical or other information is NOT sufficient authorization for the release for further disclosure."

Alcohol and Substance Abuse Related Confidentiality Restrictions:

Alcohol and substance abuse information is confidential pursuant to 42 C.F.R. Part 2. General authorizations are ineffective to obtain the release of such data. The federal regulations provide for a specific release for such data.

Term and Termination

(a) Termination for cause under HIPAA or HI-TECH. The Term of this Section shall be as described elsewhere in the "Term" section of the Contract. Among the other reasons for which ITS may terminate the Contract prior to the end of its Term date for cause, ITS may terminate the Contract if ITS determines the Contractor or its Subcontractor(s) have violated a material term of this HIPAA and HI-TECH Compliance Section of the Contract, and Contractor or its Subcontractor(s) have not cured the breach or ended the violation within any time that has been specified by ITS.

(b) Contractor's and its Subcontractor(s)' Obligations Upon Termination. Upon termination of the Contract for any reason, Contractor and its Subcontractor(s) shall return to ITS, transfer to another of ITS' contractors as directed by ITS, or, if agreed to by ITS on an individual case-by-case basis, destroy all protected health information received from ITS, or created, maintained, or received by the Contractor and its Subcontractor(s) on behalf of ITS, that the Contractor and its Subcontractor(s) still maintain in any form. Contractor and its Subcontractor(s) shall retain no copies of the protected health information. Contractor understands and agrees and will require of its Subcontractor(s) in writing that Contractor and its Subcontractor(s) are required to receive written approval from ITS prior to the return, transfer, or destruction of any protected health information.

(c) Survival. Contractor's and its Subcontractor(s)' obligations under this HIPAA and HI-TECH Compliance section of the Contract shall survive the termination of the Contract.

Miscellaneous

(a) Regulatory References. A reference in the Contract to a section in the HIPAA or HI-TECH Rules means the section as in effect or as amended.

(b) Amendment. The Parties agree to take such action as is necessary to amend the Contract from time to time as is necessary for compliance with the requirements of the HIPAA or HI-TECH Rules and any other applicable law.

(c) Interpretation. Any ambiguity in the Contract shall be interpreted to permit compliance with the HIPAA or HI-TECH Rules.

(d) Sub-contractors. Contractor shall require any Subcontractors that it uses that create, receive, maintain, or transmit protected health information on behalf of ITS under the Contract to conform to these HIPAA and HI-TECH Compliance requirements in addition to any other security, privacy, or applicable terms of the Contract.

D. QUESTIONS

All questions shall be emailed to the Designated Contact E-Mail Address indicated on the Cover Page of this RFQ.

Contractors are strongly encouraged to submit questions as early as possible. However, all questions must be submitted by the Question due date and time listed on the Cover Page of this RFQ. Answers to all questions of a substantive nature shall be provided to all Contractors who received this RFQ in the form of a question-and-answer document.

All Bids must conform to the terms set forth in this RFQ and the OGS Information Technology Umbrella Contract – Manufacturer Based. Extraneous terms or material deviations (including additional, inconsistent, conflicting, or alternative terms) may render the Bid non-responsive and may result in rejection of the Bid. Extraneous terms submitted on standard, pre-printed forms (including but not limited to product literature, order forms, license agreements, contracts, or other documents) that are attached or referenced with submissions shall not be considered part of the Bid or Authorized User Agreement but shall be deemed included for informational or promotional purposes only.

Each proposed extraneous term must be specifically enumerated in writing and specify the section of this RFQ that Bidder proposes to modify and the reasons why. Any extraneous terms must be submitted during the Question-and-Answer period as listed on the Cover Page of this RFQ. Extraneous terms submitted after this time will not be considered.

No extraneous term shall be incorporated into the Authorized User Agreement unless expressly accepted by ITS in writing. Acceptance and/or processing of a Bid shall not constitute acceptance of extraneous terms.

E. DOWNSTREAM PROHIBITION

None.

F. AUTHORIZED USER DISPUTE RESOLUTION PROCESS

Should a dispute or protest arise regarding this RFQ, the dispute or protest will be considered and decided by the Authorized User.

1. Disputes or Controversies Occurring During the Term of the Authorized User Agreement.
In the event there is a dispute or controversy during the term of the Authorized User Agreement resulting from this RFQ, the Contractor and Authorized User agree to exercise their best efforts to resolve the dispute as soon as possible. The Contractor and Authorized User shall, without delay, continue to perform their respective obligations under the resulting Authorized User Agreement and this Centralized Contract which are not affected by the dispute. Primary responsibility for resolving any dispute arising under the Authorized User Agreement shall rest with the persons designated by the Authorized User and the Contract's Contract Administrator and/or Account Manager.

In the event the Authorized User is dissatisfied with the Contractor's Products provided under the Authorized User Agreement, the Authorized User shall notify the Contractor in writing pursuant to the terms of the Contract. In the event the Contractor has any disputes with the Authorized User, the Contractor shall so notify the Authorized User in writing. If either party notifies the other of such dispute or controversy, the other party shall then make good faith efforts to solve the problem or settle the dispute amicably, including meeting with the party's representatives to attempt diligently to reach a satisfactory result.

If negotiation between such persons fails to resolve any such dispute to the satisfaction of the parties within fourteen (14) business days or as otherwise agreed to by the Contractor and Authorized User, of such notice, then the matter shall be submitted to the persons designated by the Authorized User and the Contractor's senior officer of the rank of Vice President or higher as its representative. Such representatives shall meet in person and shall attempt in good faith to resolve the dispute within the next fourteen (14) business days or as otherwise agreed to by the parties. This meeting must be held before either party may seek any other method of dispute resolution, including judicial or governmental resolutions. Notwithstanding the foregoing, nothing in this section shall be construed to prevent either party from seeking and obtaining temporary equitable remedies, including injunctive relief.

The Contractor shall extend the dispute resolution period for so long as the Authorized User continues to make reasonable efforts to cure the breach, except with respect to disputes about the breach of payment of fees or infringement of its or its licensors' intellectual property rights.

G. RESERVED RIGHTS

Bidders are hereby notified that New York State reserves the right to:

1. Reject any or all Bids received in response to the solicitation.
2. Withdraw the solicitation at any time, at the Agency's sole discretion.
3. Make an award under the solicitation in whole or in part.
4. Disqualify any Bidder whose conduct and/or Bid fails to conform to the requirements of the solicitation.
5. Seek clarifications and revisions of Bids.
6. Prior to the Bid deadline, amend the solicitation requirements to correct errors or oversights, or to supply additional information, as it becomes available.
7. Prior to the Bid deadline, direct Bidders to submit Bid modifications addressing subsequent solicitation amendments.
8. Change any of the schedule dates with timely notification to all prospective Bidders.
9. Eliminate any mandatory, non-material specifications that cannot be complied with by all of the prospective Bidders.
10. Waive any requirements that are not material.
11. Utilize any and all ideas submitted in the Bids received.
12. Negotiate with the Bidder responding to the solicitation within the solicitation requirements to serve the best interests of the State. This includes requesting increased discounts and clarifications of any or all Bidder's' Bids.
13. Require clarification at any time during the procurement process and/or require correction of arithmetic or other apparent errors for the purpose of assuring a full and complete understanding of a Bidder's Bid and/or to determine a Bidder's compliance with the requirements of the solicitation; and
14. Select and award to other than the selected Bidder(s) in the event of unsuccessful negotiations or, optionally, in other specified circumstances as detailed in the solicitation requirements.

15. Purchase none, some, all or more of the quantities of the items listed in Attachment 1 under this RFQ.
16. If applicable, consultants will be required to comply with ITS policies and procedures; pass background checks; and sign non-disclosure agreements.
17. If applicable, vendors may be required to complete Form A – Consultant Disclosure Form.
18. Extend the term of this agreement in accordance with the above outlined solicitation.

Manufacturer / Authorized Reseller Information

This Page is to be Completed By the Manufacturer or Authorized Reseller Responding to the RFQ

The RFQ Response must be fully and properly executed by an authorized person. By signing you certify your express authority to sign on behalf of yourself, your company, or other entity and full knowledge and acceptance of this RFQ (including any Questions/Answers or addenda), the OGS Centralized Contract and that all information provided is complete, true and accurate. Quotes received by RFQ due date/time are binding and non-retractable for 120 days or as stipulated in the RFQ.

Contract #	Manufacturer Name	Authorized Reseller Name
TS-2024-526DB	Google	Protek

Manufacturer or Reseller Signature: Jill Pittore *Date:* 11-05-24	*Phone Number:* *E-Mail:* jill@protek.io
Printed or Typed Name: Jill Pittore, President	*Title:*

If you are not providing a RFQ Response, place an "x" in the box, please explain why you are not responding, and return this page only.

☐ WE ARE UNABLE TO RESPOND AT THIS TIME BECAUSE:

After fully completing the information above, please submit this page via e-mail with "Request for Quote – Financial Response – Cloud Solution" (Excel) to the Authorized User indicated on the Cover Page. Authorized User reserves the right to request the original executed page of this RFQ.

Request for Quote - Financial Response - Cloud Solution

RFQ Number	Authorized User Name	Contract Number	Manufacturer / Reseller Name	Date Completed	Grand Total
ITS-2024-526DB-Google Cloud SA	Information Technology Services (ITS)	PM67982	Google/Protek	11/5/2024	$44,539,305.00

Unanticipated Enhancements to Services is only applicable to items in Lot 4 - Implementation Services and is calculated based on the percentage the Authorized User chooses in cell E7 (not to exceed 20%).

Unanticipated Enhancements to Services (Not to Exceed 20%)	Implementation Base Total (*without* Unanticipated Enhancements)	Implementation Total (*with* Unanticipated Enhancements)	Recurring Cost Total	Data Transfer Cost Total
0%	$0.00	$0.00	$44,539,305.00	$0.00

Please See Request for Quotes for all Authorized User requirements.

Lot this RFQ Applies to: ☐ Lot 1 Software ☐ Lot 2 Hardware ☑ Lot 3 Cloud ☐ Lot 4 Implementation

If the RFQ includes Lot 4 – Implementation, Contractor must prior to submitting a response to the RFQ either hold an award for Lot 4- Implementation, or be able to provide the services under the other Lots included in the RFQ.

Instructions for When SKU's Have Been Identified by Authorized User

Authorized User will complete RFQ Number, Authorized User Name, Unanticipated Enhancements to Services Percent, Deliverable Number, Deliverable Name, Lot Number, Product Description(s), Manufacturer Part Number(s) (SKU), Net NYS Contract Price(s) and Qty, and Data Transfer Specifications in each of the three sections: Implementation Items, Recurring Items, and Data Transfer Items. The totals of each of these three sections will calculate into the Total Deliverable Cost. Please note, any anticipated deliverable travel costs are only applicable to items in Lot 4 - Implementation Services.
Manufacturer / Reseller will complete Deliverable Narrative, Additional Product Discount (Percentage), and optional Additional Product Discount (Dollars).

Instructions for When Authorized User Requires Vendor to Provide Suggested SKU's

Authorized User will complete RFQ Number and Authorized User Name, Unanticipated Enhancements to Services Percent, and Data Transfer Specifications in each of the three sections: Implementation Items, Recurring Items, and Data Transfer Items. The totals of each of these three sections will calculate into the Total Deliverable Cost. Please note, any anticipated deliverable travel costs are only applicable to items in Lot 4 - Implementation Services.
Manufacturer / Reseller will complete Deliverable Number, Deliverable Name, Deliverable Narrative, Lot Number, Product Description, Manufacturer Part Number (SKU), Net NYS Contract Price, Additional Product Discount (Percentage), Qty and optional Additional Product Discount (Dollars) to meet a defined need as detailed in the Authorized User Request for Quote.
RESPONSES ARE BINDING AND NON-RETRACTABLE

Deliverable Information

Deliverable Number	Deliverable Name

Implementation Items

RFQ Item Number	Lot Number	Product Description	Manufacturer Part Number (SKU)	Net NYS Contract Price	Additional Product Discount (Percentage)	RFQ Product Price	Qty	Additional Product Discount (Dollars)	Extended RFQ Price	Unanticipated Enhancements to Services (Not to Exceed 20%)
1										
2										
3										
4										
5										
								Anticipated Deliverable Travel Costs (Lot 4 - Implementation Services only)		$0.00
								Total Deliverable Implementation Cost	$0.00	$0.00

RFQ Number	Authorized User Name	Contract Number	Manufacturer / Reseller Name	Date Completed	Grand Total
ITS-2024-526DB-Google Cloud SA	Information Technology Services (ITS)	PM67982	Google/Protek	11/5/2024	$44,539,305.00

Unanticipated Enhancements to Services is only applicable to items in Lot 4 - Implementation Services and is calculated based on the percentage the Authorized User chooses in cell E7 (not to exceed 20%).

Unanticipated Enhancements to Services (Not to Exceed 20%)	Implementation Base Total (*without* Unanticipated Enhancements)	Implementation Total (*with* Unanticipated Enhancements)	Recurring Cost Total	Data Transfer Cost Total
0%	$0.00	$0.00	$44,539,305.00	$0.00

Please See Request for Quotes for all Authorized User requirements.

Recurring Items

RFQ Item Number	Lot Number	Product Description	Manufacturer Part Number (SKU)	Net NYS Contract Price	Additional Product Discount (Percentage)	RFQ Product Price	Qty	Additional Product Discount (Dollars)	Extended RFQ Price
		Year One - Term Dates to be determined							
1	Lot 3	Enterprise Agreement for Public Sector Subscription Used for a fixed price offering (not pay-as-you-go) with quantity calculated by Google up front for 1, 2, or 3 years. Prepaid with no true ups required during the 1, 2, or 3 year period covered by the fixed price. Includes unlimited Google Cloud access, but is not an aggregate of skus, and not on a per seat license basis. No professional services included. Not maintenance or support of other Google Cloud Products. Not a customer-specific sku but instead available to all public sector customers (listed on Google's Manufacturer's Price List with a list Price).	9A92-40AE-8D00	$0.99			8728507.00		$0.00
2	Lot 3	GCP Points-Access to all GCP Solutions-Compute, Storage & Databases, Networking, Big Data Data Transfer, Machine Learning, APIs, IoT, Management, Developer and Security Tools- Payment-Monthly based Usage	G-POINTS-MON	$0.99			5588297.00		$0.00
3	Lot 3	Bytes of data ingested in US for the Enterprise Plus package under subscription	70CB-8A2E-163E	$4.51			800000.00		$0.00
4	Lot 3	Monthly BeyondCorp Enterprise Users (Month) Qty 114,000 times 12 months = 1,368,000	E2D2-474B-B4EF	$5.88			1368000.00		$0.00
5	Lot 3	Platform Elite - Customer Hosted - Looker by Google Qty 5 times 12 months = 60	Looker-105	$14,700.00			60.00		$0.00
6	Lot 3	GCP Support Base - Region 1 countries Qty 4 times 12 months = 48	SUPPORT-GCP-BASE-PREM-REG1	$12,250.00			48.00		$0.00
		Year Two- Term Dates to be determined							
7	Lot 3	Enterprise Agreement for Public Sector Subscription Used for a fixed price offering (not pay-as-you-go) with quantity calculated by Google up front for 1, 2, or 3 years. Prepaid with no true ups required during the 1, 2, or 3 year period covered by the fixed price. Includes unlimited Google Cloud access, but is not an aggregate of skus, and not on a per seat license basis. No professional services included. Not maintenance or support of other Google Cloud Products. Not a customer-specific sku but instead available to all public sector customers (listed on Google's Manufacturer's Price List with a list Price).	9A92-40AE-8D00	$0.99			9322032.00		$0.00
8	Lot 3	GCP Points-Access to all GCP Solutions-Compute, Storage & Databases, Networking, Big Data Data Transfer, Machine Learning, APIs, IoT, Management, Developer and Security Tools- Payment-Monthly based Usage	G-POINTS-MON	$0.99			5983980.00		$0.00
9	Lot 3	Bytes of data ingested in US for the Enterprise Plus package under subscription	70CB-8A2E-163E	$4.51			800000.00		$0.00
10	Lot 3	Monthly BeyondCorp Enterprise Users (Month) Qty 114,000 times 12 months = 1,368,000	E2D2-474B-B4EF	$5.88			1368000.00		$0.00
11	Lot 3	Platform Elite - Customer Hosted - Looker by Google Qty 5 times 12 months = 60	Looker-105	$14,700.00			60.00		$0.00
12	Lot 3	GCP Support Base - Region 1 countries Qty 4 times 12 months = 48	SUPPORT-GCP-BASE-PREM-REG1	$12,250.00			48.00		$0.00
13									
14									
15									
								Total Deliverable Recurring Cost	$44,539,305.00

RFQ Number	Authorized User Name	Contract Number	Manufacturer / Reseller Name	Date Completed	Grand Total
ITS-2024-526DB-Google Cloud SA	Information Technology Services (ITS)	PM67982	Google/Protek	11/5/2024	$44,539,305.00

Unanticipated Enhancements to Services is only applicable to items in Lot 4 - Implementation Services and is calculated based on the percentage the Authorized User chooses in cell E7 (not to exceed 20%).

Unanticipated Enhancements to Services (Not to Exceed 20%)	Implementation Base Total (*without* Unanticipated Enhancements)	Implementation Total (*with* Unanticipated Enhancements)	Recurring Cost Total	Data Transfer Cost Total
0%	$0.00	$0.00	$44,539,305.00	$0.00

Please See Request for Quotes for all Authorized User requirements.

Data Transfer Items

Data Transfer Specifications:

RFQ Item Number	Lot Number	Product Description	Manufacturer Part Number (SKU)	Net NYS Contract Price	Additional Product Discount (Percentage)	RFQ Product Price	Qty	Additional Product Discount (Dollars)	Extended RFQ Price	Unanticipated Enhancements to Services (Not to Exceed 20%)
1										
2										
3										
4										
5										
								Anticipated Deliverable Travel Costs (Lot 4 - Implementation Services only)		
								Total Deliverable Data Transfer Cost	$0.00	$0.00

Total Deliverable Cost	$44,539,305.00

Google Cloud Terms, Conditions and Clarifications
The resulting orders and agreement are subject to the previously agreed terms between Google LLC and New York, as well as Google's terms specific to Period Recruitment 2 pursuant to Section 28 of Appendix B, available at the following link:
https://static.carahsoft.com/concrete/files/2616/8683/8769/Google_Cloud_Agreement_with_Period_Recruitment_2_-_Updated.pdf
Subscription Period: the period starting on the Implementation Date and continuing for twenty-four (24) months during which Customer may use the Subscription Services.
Enterprise Agreement for Public Sector Subscription (GCP Subscription) may only be used for the below Qualifying Workload.
Qualifying Workload:
The following services may be used to implement the Project (defined below) during the Subscription Period:
1. The Google Cloud Platform products (excluding the products listed below, subject to the Restrictions).
"Project" means centralized ITS cloud computing environment for New York State Agencies.
"Restrictions" means the following restrictions or assumptions applicable to the Project:
1. The product for Google Chrome Enterprise Premium (Google Beyond Corp) is limited to 114,000 individuals in the state
2. The product Chronicle is limited to 800,000 GB of storage
3. Subscription is for a period of 24 months for the workloads of New York State covered by ITS.
4. The subscription does not cancel or supersede any existing Subscription Agreements between New York State and Google Public Sector.
5. The workload excludes Medicaid workloads unless agreed upon with Google Public Sector team
6. Utilization of the Google Cloud Platform Products under the Subaccount during any consecutive 12 months will not exceed in the aggregate $28,600,000.00 USD based on Google's then-current list price, minus any discounts applicable to the Subaccount ("Utilization Cap"). Upon reaching the Utilization Cap at any time of the Subscription Period, any unpaid portion of fees for line items 1-12 shall become due and the parties shall work in good faith to negotiate and execute a new subscription agreement. If the parties fail to reach agreement on a new subscription within 30 days of exceeding the Utilization Cap, Carahsoft may, in its sole discretion, terminate this Agreement. Carahsoft will invoice Customer for the remaining unpaid portion of line items 1-12, and Customer will pay the invoiced amount in accordance with the payment terms in the Agreement. Carahsoft does not waive its right to claim payment for any unpaid portion of line items 1-12 by not exercising or delaying the exercise of any rights under this Section.

RFQ Number	Authorized User Name	Contract Number	Manufacturer / Reseller Name	Date Completed	Grand Total
ITS-2024-526DB-Google Cloud SA	Information Technology Services (ITS)	PM67982	Google/Protek	11/5/2024	$44,539,305.00

Unanticipated Enhancements to Services is only applicable to items in Lot 4 - Implementation Services and is calculated based on the percentage the Authorized User chooses in cell E7 (not to exceed 20%).	Unanticipated Enhancements to Services (Not to Exceed 20%)	Implementation Base Total (*without* Unanticipated Enhancements)	Implementation Total (*with* Unanticipated Enhancements)	Recurring Cost Total	Data Transfer Cost Total
	0%	$0.00	$0.00	$44,539,305.00	$0.00

Please See Request for Quotes for all Authorized User requirements.

7. A 3rd year option to extend SA at mutual agreed upon amount
The order does not include:
1. Apigee (Subscription-based);
2. Appsheet;
3. Google Workspace;
4. Marketplace Offerings;
5. GCP products that require separate subscriptions;
6. Bare Metal Solution;
7. Maps or Maps API services; and
8. any third party solutions used by the Customer in connection with the Project.
1. Additional Definitions.
A. "Implementation Date" means no later than 5 business days after the Agreement Effective Date.
B. "List Price" means the then-current prices for the applicable Google Cloud Platform products described at Google Products or a successor URL.
C. "Qualifying GCP products" means the Google Cloud Platform products listed here (Google Products) that Customer may use under the Subaccount for the implementation of the Qualifying Workload, excluding Google Cloud Platform.
D. "Qualifying Workload" means the project approved by Google for Customer to use the Qualifying GCP products.
2. Restrictions. Customer's use under the Subaccount of (i) any Google Cloud Platform product that is not a Qualifying GCP product or (ii) any Qualifying GCP product for any purpose other than to implement the Qualifying Workload (each, an "Unqualified Use"), is not permitted.

Cover Page – Request for Quote – Cloud Solution

TO BE COMPLETED BY AUTHORIZED USER

RFQ Title **Google Cloud SA** **RFQ Number** ITS-2024-526DB

Authorized User Information:
Office of Information Technology Services
Empire State Plaza
Swan Street Building, Core 4
2nd Floor, Room 2404
Albany, NY 12223

Authorized User Delivery Information:
Joseph Marshall
NYS Office of Information Technology Services
Swan Street Bldg, Core 4, Floor 3
Empire State Plaza
Albany, NY 12227

Special Delivery Instructions:

DESIGNATED CONTACTS

Name(s)	E-Mail(s)
Dominic Brefo – Contract Manager	Its.sm.ITS_BIDS@its.ny.gov

Authorized User shall indicate if Procurement Lobbying Law/Restricted Period is in effect: ☒ **Yes** ☐ **No**
Where Procurement Lobbying Law is deemed applicable by the Authorized User, by signing, Contractor affirms that it understands and agrees to comply with the Authorized User's policies and procedures relative to permissible contacts. Information may be accessed at: Procurement Lobbying:
http://www.ogs.ny.gov/aboutOgs/regulations/defaultAdvisoryCouncil.html)

RFQ LOTS

This RFQ is for Products from the following checked Lots as defined in Award # 22802 – Information Technology Umbrella Contract – Manufacturer Based (Statewide):

☐ Lot 1 – Software ☐ Lot 2 – Hardware ☒ Lot 3 - Cloud ☐ Lot 4 – Implementation

The Authorized User named above is seeking competitive quotes from the Contractor (Manufacturer) and their Resellers (where applicable) of Information Technology Umbrella Contract – Manufacturer Based Contract(s) for the above-referenced Products. If the RFQ includes Lot 4 – Implementation, Contractor must prior to submitting a response to the RFQ either hold an award for Lot 4- Implementation or be able to provide the services under the other Lots included in the RFQ.

LOT 3 – CLOUD DATA RISK LEVEL: ☐ Low ☒ Medium ☐ High

DATA CATEGORIZATION ELEMENTS: Data is all public information.

QUESTIONS AND OTHER EVENTS

Event	Date	Time
RFQ Release Date	11/1/2024	N/A
Questions Due	11/4/2024	3:00 PM EST
Vendor Response Due Date	11/5/2024	3:00 PM EST

IS THE RFQ BIDDER POOL LIMITED TO M/WBE, SB, AND SDVOB VENDORS: ☐ Yes ☒ No

BASIS FOR AWARD
☒ Lowest Price Meeting Specified Technical Requirements
☐ Lowest Price Meeting Specified Technical Requirements **and** Mandatory Pass/Fail Requirements
☐ Best Value with Technical and Financial Score

E-RATE ELIGIBLE ☐ Yes (E-Rate Discounts are Required) ☒ No

SERVICE MODEL FOR LOT 3 – CLOUD SOLUTION *(check all that apply)*
☒ Software as a Service (SaaS)
☒ Platform as a Service (PaaS)
☒ Infrastructure as a Service(IaaS)
☐ Anything as a Service (XaaS)

DEPLOYMENT MODEL FOR LOT 3 – CLOUD SOLUTION (*Check all that apply*)	☐ Private Cloud ☐ Community Cloud ☒ Public Cloud ☐ Hybrid Cloud ☐ Other
APPLICABLE STATUTORY / POLICY REQUIRMENT	☐ None ☒ CJIS ☐ FERPA ☒ FISMA ☒ GLB ☐ HIPAA ☐ HITECH ☐ Tax ☐ PPI ☐ PCI DSS ☐ SOX ☐ ECPA ☐ Other
CAIQ REQUIRMENT	☐ Yes ☒ No
ATTACHMENTS	Attachment 1 - Request for Quote – Financial Response – Cloud Solution Attachment 2 – Non-Collusive Bidding Certification Exhibit 1 – Google Master Terms and G Suite Service Schedule

The Authorized User will not be held liable for any cost incurred by the Contractor for work performed in the preparation of a response to this RFQ or for any work performed prior to the formal execution of an Authorized User Agreement. Responses to the RFQ must be received by the deadline specified above. Contractors assume all risks for timely, properly submitted deliveries. A Contractor is strongly encouraged to arrange for delivery of RFQ responses prior to the date of the RFQ opening. LATE RFQ responses may be rejected. The received time of a RFQ response will be determined by the Authorized User.

All purchases resulting from this RFQ shall be in accordance with terms and conditions of the OGS Information Technology Umbrella Contract – Manufacturer Based Contract and any additional terms and conditions set forth in this RFQ and its Attachments.

A. SCOPE / MANDATORY REQUIREMENTS

This RFQ is being distributed to the Contractor and Resellers (where applicable) to acquire the following:

1. SCOPE

This RFQ is seeking to acquire Google cloud data acquisition, compute, cybersecurity, and support products off Office of General Services centralized Google contract PM67982. These products will be used to provide centralized IT consolidation of agency contracts, satisfy existing agency demand and result in significant savings to the state thru centralization.

The term of this agreement is two years with the option to renew based upon mutual consent. Annual purchase orders will be issued. Payment of invoices will be made for actual usage on a monthly basis.

For the duration of an Authorized User Agreement, the Cloud Solution shall conform to the Cloud Solution Manufacturer's specifications, Documentation, performance standards (including applicable license terms, warranties, guarantees, Service Level Agreements, service commitments, and credits).

2. CLOUD SERVICE MODEL

Software as a Service (SaaS)
Infrastructure as a Service (IaaS)
Platform as a Service (PaaS)

3. CLOUD DEPLOYMENT MODEL

Public Cloud (Google Cloud Platform).

4. DATA CATEGORIZATION

Risk Level: Medium. All data is public information.

5. DATA OWNERSHIP

The Authorized User shall own all right, title and interest in Data.

6. DATA LOCATION

All Data shall remain in CONUS.

7. ENCRYPTION

Contractor shall use appropriate means to preserve and protect State Data. This includes, but is not limited to, use of stable storage Media, regular data backups and archiving, password protection of volumes, and data encryption. Encryption at rest as well as Encryption in flight within the Google Cloud infrastructure. Availability to leverage CMEK (Customer Managed Encryption Keys). All Data transmitted between ITS and the Contractor must comply with NYS ITS Standard NYS-S14-007 Encryption Standard (http://its.ny.gov/document/encryption-standard).

8. SECURITY

The Contractor and its personnel shall adhere to all required compliance domains, State security policies, procedures, and directives currently existing or implemented during the term of the Contract. These compliance domains and security policies include, but are not limited to, the following New York State Information Security Policies and Standards, National Institute of Standards and Technology (NIST) Policies (or their successor policies), and statutes:

P03-002 - Information Security Policy
P08-001 - Enterprise Plan to Procure Policy
P08-005 - Accessibility of Web-Based Information and Application
S13-002 - Information Classification Standard
S13-003 - Sanitation/Secure Disposal
S13-005 - Cyber Incident Response Standard
S14-002 - Information Classification Standard
S14-003 - Information Security Controls
S14-006 - Authentication Tokens Standard
S14-007 - NYS Encryption Standard

S14-010 - Remote Access
NIST Federal Information Processing Standard (FIPS) Publication 140-2
NIST Federal Information Processing Standards (FIPS) Publication 199 – Standards for Security Categorization of Federal Information and Information Systems
NIST Special Publication 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations.
NIST Special Publication 800-57, Part 1 - Recommendation for Key Management – Part 1: General
NIST Special Publication 800-088r1 - Guidelines for Media Sanitization
NIST Special Publication 800-111 - Guide to Storage Encryption Technologies for End User Devices
NIST Special Publication 800-122 - Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
NIST Special Publication 800-131A - Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths
New York State Information Security Controls Standard
New York State Risk Management Standard
Health Insurance Portability and Accountability Act of 1996

Requires implementation of Assured Workloads to meet FedRAMP Moderate compliance requirements.

CAIQ Requirement/Contractor Security:

- A Consensus Assessment Initiative Questionnaire (CAIQ) is required to be submitted by the Contractor.
- NYS ITS is retaining the right to request the CAIQ be completed annually.
- A written description of Contractor's physical/virtual security and/or internal control processes are required.
- Security Logs and Reports will need to be provided in a format communicated by NYS ITS.
- At the sole discretion of ITS, ITS may accept other audited reports in lieu of the CAIQ, provided the report meets all other requirements in this section.

The contractor warrants, covenants, and represents that it shall comply fully with all applicable ITS Information Security policies and procedures located at https://its.ny.gov/eiso/policies/security during the performance of the resulting Contract. The State may terminate the Contract if it determines that Contractor has violated a material term of this section. The terms of this section shall apply equally to Contractor, officers, agents, employees, and Subcontractors, if any. Contractor agrees that all officers, agents, employees, and Subcontractors, if any, shall be made aware of and shall agree to the terms of this section.

9. MAINTENANCE/SUPPORT

Vendor shall provide maintenance and support based on its usual commercial processes.

10. INFRASTRUCTURE SUPPORT SERVICES

Infrastructure support services that do not directly or indirectly access Data may be provided in a Follow the Sun format.

11. BUSINESS CONTINUITY/DISASTER RECOVERY (BC/DR) OPERATIONS

The Contractor must provide proof of their redundant 24x7 model including site load balancing and disaster recovery. Redundancy should span at least two highly available, secure data centers in the continental United States with a minimum of 500 miles of geographic separation. Minimum availability criteria include power supply, redundant Internet connectivity with multiple providers, fire protection, etc. Maintain full off-site back-up of operating systems, software, configurations, and any data needed to successfully recover from any hardware, software, or site failure. Disaster recovery must be tested annually.

12. AUTHENTICATION TOKENS

Authentication Tokens are required and must meet the AAL1 standard as a minimum.

13. APPLICATION PROGRAM INTERFACE (API) OR SELF ELECTRONIC PORTAL

New York State requires access to both an API and electronic portal for the purposes of accessing, downloading, and/or interacting with data within the system.

B. STATEMENT OF WORK

This is an enterprise agreement subscription and as such there is no statement of work for the contractor.

1. IMPLEMENTATION OF CLOUD SOLUTION

N/A

2. RECURRING SERVICES

The items listed in the Attachment 1.

3. TRANSFER OF DATA

N/A

Contractor cannot charge for the transfer of Data unless the charges are provided for in response to this RFQ.

C. AUTHORIZED USER TERMS AND CONDITIONS

1. DATA BREACH – REQUIRED CONTRACTOR ACTIONS

Unless otherwise provided by law, in the event of a Data Breach, the Contractor shall:
1. Notify the ITS and any potentially affected Authorized User(s), or their designated contact person(s), by telephone as soon as possible, but in no event more than 12 hours from the time the Contractor confirms the Data Breach.
2. Consult with and receive authorization from the Authorized User as to the content of any notice to affected parties prior to notifying any affected parties to whom notice of the Data Breach is required, either by statute or by the Authorized User.
3. Coordinate all communication regarding the Data Breach with the ITS and Authorized User (including possible communications with third parties).
4. Cooperate with the Authorized User, ITS and any Contractor working on behalf of the Authorized User or ITS in attempting (a) to determine the scope and cause of the breach; and (b) to prevent the future recurrence of such security breaches; and
5. Take such corrective actions that the Contractor deems necessary to contain the Data Breach. Contractor shall provide Written notice to the Authorized User as to all such corrective actions taken by the Contractor to remedy the Data Breach. Unless otherwise agreed to in the Authorized User Agreement, if Contractor is unable to complete the corrective action within the required timeframe, the remedies provided in Appendix B, Section 52, Remedies for Breach shall apply and (i) the Authorized User may contract with a third party to provide the required services until corrective actions and services resume in a manner acceptable to the Authorized User, or until the Authorized User has completed a new procurement for a replacement service system; (ii) and the Contractor will be responsible for the reasonable cost of these services during this period.

Nothing herein shall in any way (a) impair the Authorized User or OAG to bring an action against Contractor to enforce the provisions of the New York State Information Security Breach Notification Act (ISBNA) or (b) limit Contractor's liability for any violations of the ISBNA or any other applicable statutes, rules, or regulations.

2. AUTHORIZED USER ACCESS TO DATA

The Authorized User shall have access to its Data at all times, through the term of the Authorized User Agreement.

The Authorized User shall have the ability to import or export Data in piecemeal or in its entirety at the Authorized User's discretion at no charge to the Authorized User. This includes the ability for the Authorized User to import or export Data to/from other Contractors.

3. CONTRACTOR ACCESS TO DATA

The Contractor shall not copy or transfer Data unless authorized in writing by the Authorized User. In such an event the Data shall be copied and/or transferred in accordance with the provisions of this Section. Contractor shall not access any Data for any purpose other than fulfilling the service. Contractor is prohibited from Data Mining, cross tabulating, monitoring Authorized User's Data usage and/or access, or performing any other Data analytics other than those required within the Authorized User Agreement. At no time shall any Data or processes (e.g. workflow, applications, etc.), which either are owned or used by the Authorized User be copied, disclosed, or retained by the Contractor or any party related to the Contractor. Contractors are allowed to perform industry standard back-ups of Data. Documentation of back-up must be provided to the Authorized User upon request. Contractor must comply with any and all security requirements within the Authorized User Agreement.

4. SUSPENSION OF SERVICES

During any period of suspension of service, the Authorized User shall have full access to all Data at no charge. The Contractor shall not take any action to erase and/or withhold any Authorized User Data, except as directed by the Authorized User.

5. EXPIRATION OR TERMINATION OF SERVICES

Upon expiration or termination of an Authorized User Agreement, the Authorized User shall have full access to all Data for a period of 60 calendar days. During this period, the Contractor shall not take any action to erase and/or withhold any Data, except as directed by the Authorized User. An Authorized User shall have the right to specify a period more than 60 calendar days in its RFQ. There will be no additional charge to the State for this access.

6. ACCESS TO SECURITY LOGS AND REPORTS

Upon request, the Contractor shall provide access to security logs and reports to the State or Authorized User in a format as specified by the Authorized User.

7. CONTRACTOR PERFORMANCE AUDIT

The Contractor shall allow the Authorized User to assess Contractor's performance by providing any materials requested in the Authorized User including but not limited to page load times, response times, uptime, and fail over time. The Authorized User may perform this Contractor performance audit with a third party at its discretion, at the Authorized User's expense.

The Contractor shall perform an independent audit of its Data Centers, at least annually, at Contractor expense. The Contractor will provide a data owner facing audit report upon request by the Authorized User. The Contractor shall identify any confidential, trade secret, or proprietary information in accordance with Appendix B, Section 9(a), Confidential/Trade Secret Materials.

Except as otherwise provided for, all status reports and other documents produced for the State become the property of the State.

8. MODIFICATION TO CLOUD SERVICE DEPLOYMENT MODEL, SERVICE MODEL, AND/OR INITIAL FUNCTIONALITY WITHIN AN AUTHORIZED USER AGREEMENT

As Cloud services, can be flexible and dynamic, delivery mechanisms may be subject to change. This may result in changes to the deployment model, service model, functionality, or SKU. The OGS and Authorized Users require notification of any such changes to ensure security and business needs are met.

Any changes to the deployment model, service model, functionality, or SKU (e.g., PaaS to IaaS) must be provided to OGS via Appendix C - Contract Modification Procedures.

In addition, notification must be provided to the Authorized User for review and acceptance, prior to implementation. Any changes to the Authorized User Agreement will require the Authorized User to re-assess the risk mitigation methodologies and strategies and revise the Authorized User Agreement as needed.

9. BACKGROUND CHECK REQUIREMENTS

All Contractor Staff shall, prior to the commencement of any services pursuant to this RFQ, whether on or off-site, comply with all State onboarding and security clearance requirements, including training and signing certifications or agreements, required for access to NYS Confidential Information or Data or required for access to NYS Facilities or Data Centers, the preceding described, collectively, as "onboarding." This includes requirements related to the access to Regulated data, including any requirements of the State's public safety agencies, or those related to the Federal Bureau of Investigation Criminal Justice Information Services (CJIS) Security Policy (https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center).

Contractor agrees that its Contractor Staff performing services on-site at NYS Facilities or Data Centers or those with logical access to NYS Confidential Information or Data (i.e., log-in access) shall be required to undergo the same security clearances as those required of ITS employees. If not physically or virtually escorted, each Contractor Staff designated to work under the Authorized User Agreement with ITS shall submit identifying information to the State and be fingerprinted. ITS shall arrange for the scheduling of fingerprinting. Such fingerprints shall be submitted to the NYS Division of Criminal Justice Services for a state criminal history record check and, at ITS' discretion, to the Federal Bureau of Investigation for a national criminal history record check.

Contractor also agrees that its Contractor Staff performing services on-site at NYS Facilities or Data Centers may be required to comply with those health checks which NYS requires of its own employees working on-site including for example providing proof of vaccination against, and/or testing for, infectious disease such as COVID-19.

All expenses, including travel and lodging, associated with the onboarding and security clearance process including fingerprinting of Contractor Staff are the responsibility of the Contractor and are not reimbursable.

ITS shall make all suitability determinations on Contractor Staff. For purposes of this Section, a "suitability determination" is a determination that there are reasonable grounds to believe that an individual will likely be able to perform the Authorized User Agreement requirements without undue risk to the interests of the State. Failure of a security clearance or non-compliance with this Section will disqualify any Contractor Staff from performing any services on the Authorized User Agreement. If any Contractor Staff are removed from providing services under the Authorized User Agreement, they may be subject to all onboarding and security clearance requirements if they are returned to performing services under the Authorized User Agreement.

All Contractor Staff shall, at the termination of their providing services to ITS under this RFQ, comply with all State off-boarding and security procedures, including return to ITS of any physical or logical access badges or other credentials that were issued by the State and required for their access to NYS Confidential Information or Data or NYS Facilities or Data Centers.

10. ACCESS TO REGULATED DATA

The Contractor agrees to comply with the requirements listed in Appendix F for those Applicable Statutory Requirements indicated on the cover page of this RFQ. In addition to the terms found in the Contract and Appendix F, the following provisions shall apply to this RFQ.

Criminal Justice Information Services

The Contractor agrees to comply with all requirements in the most recent approved version Criminal Justice Information Services (CJIS) Security Policy, available at https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center/view and the terms of the CJIS Security Addendum below. As of the date of this RFQ, the most recent approved version of the CJIS Security Policy is Version 5.9.5, dated July 9, 2024.

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks, and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

a. Investigate or decline to investigate any report of unauthorized use.

b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer
Criminal Justice Information Services Division, FBI
1000 Custer Hollow Road
Clarksburg, West Virginia 26306

Safeguarding Federal Tax Information

I. PERFORMANCE

In performance of this Contract, the Contractor agrees to comply with and assume responsibility for compliance by Contractor Staff with the following requirements:

(1) All work will be performed under the supervision of the Contractor.

(2) The Contractor and Contractor Staff to be authorized access to Federal Tax Information (FTI) must meet the background check requirements defined in IRS Publication 1075. The Contractor will maintain a list of Contractor Staff authorized access to FTI. Such list will be provided to ITS and, upon request, to the IRS.

(3) FTI made available in any format shall be used only for the purpose of carrying out the provisions of this Contract. FTI in any format shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this Contract. Inspection by or disclosure of FTI to anyone other than the Contractor or Contractor Staff authorized is prohibited.
(4) All FTI will be accounted for upon receipt and properly stored before, during, and after processing. In addition, any related output and products will be given the same level of protection as required for the source material.
(5) The Contractor will certify that the FTI processed during the performance of this Contract will be completely purged from all physical and electronic data storage with no output to be retained by the Contractor at the time the work is completed. If immediate purging of physical and electronic data storage is not possible, the Contractor will certify that any FTI in physical or electronic storage will remain safeguarded to prevent unauthorized disclosures.
(6) Any spoilage or any intermediate hard copy printout that may result during the processing of FTI will be given to ITS. When this is not possible, the Contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts and will provide ITS with a statement containing the date of destruction, description of material destroyed, and the destruction method.
(7) All computer systems receiving, processing, storing, or transmitting FTI must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to FTI.
(8) No work involving FTI furnished under this Contract will be subcontracted without prior written approval of the IRS.
(9) Contractor will ensure that the terms of FTI safeguards described herein are included, without modification, in any approved subcontract for work involving FTI.
(10) To the extent the terms, provisions, duties, requirements, and obligations of this Contract apply to performing services with FTI, the Contractor shall assume toward the subcontractor all obligations, duties, and responsibilities that ITS under this Contract assumes toward the Contractor, and the subcontractor shall assume toward the Contractor all the same obligations, duties and responsibilities which the Contractor assumes toward ITS under this Contract.
(11) In addition to the subcontractor's obligations and duties under an approved subcontract, the terms and conditions of this Contract apply to the subcontractor, and the subcontractor is bound and obligated to the Contractor hereunder by the same terms and conditions by which the contractor is bound and obligated to ITS under this Contract.
(12) For purposes of this contract, the term "contractor" includes any officer or employee of the contractor with access to or who uses FTI, and the term "subcontractor" includes any officer or employee of the subcontractor with access to or who uses FTI.
(13) ITS will have the right to void the Contract if the Contractor fails to meet the terms of FTI safeguards described herein.

II. CRIMINAL/CIVIL SANCTIONS

(1) Each Contractor Staff of a Contractor to whom FTI is or may be disclosed shall be notified in writing that FTI disclosed to such Contractor Staff can be used only for a purpose and to the extent authorized herein, and that further disclosure of any FTI for a purpose not authorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution.
(2) Each Contractor Staff of a Contractor to whom FTI is or may be accessible shall be notified in writing that FTI accessible to such Contractor Staff may be accessed only for a purpose and to the extent authorized herein, and that access/inspection of FTI without an official need-to-know for a purpose not authorized herein constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution.
(3) Each Contractor Staff of a Contractor to whom FTI is or may be disclosed shall be notified in writing that any such unauthorized access, inspection or disclosure of FTI may also result in an award of civil damages against the Contractor Staff in an amount equal to the sum of the greater of $1,000 for each unauthorized access, inspection, or disclosure, or the sum of actual damages sustained as a result of such unauthorized access, inspection, or disclosure, plus in the case of a willful unauthorized access, inspection, or disclosure or an unauthorized access/inspection or disclosure which is the result of gross negligence, punitive damages, plus the cost of the action. These penalties are prescribed by IRC sections 7213, 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.
(4) Additionally, it is incumbent upon the Contractor to inform its Contractor Staff of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1),

which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of their employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.
(5) Granting a contractor access to FTI must be preceded by certifying that each Contractor Staff understands ITS's security policies and procedures for safeguarding FTI. The Contractor and Contractor Staff must maintain their authorization to access FTI through annual recertification of their understanding of ITS's security policy and procedures for safeguarding FTI. The initial certification and recertifications must be documented and placed in the ITS's files for review. As part of the certification and at least annually afterwards, the Contractor and each Contractor Staff must be advised of the provisions of IRC sections 7213, 7213A, and 7431 (see Exhibit 4, *Sanctions for Unauthorized Disclosure*, and Exhibit 5, *Civil Damages for Unauthorized Disclosure*). The training on ITS's security policies and procedures provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches (See Section 10). For the initial certification and the annual recertifications, the Contractor and each Contractor Staff must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. INSPECTION

The IRS and ITS, with 24-hour notice, shall have the right to send its inspectors into the offices and plants of the Contractor to inspect facilities and operations performing any work with FTI under this Contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process, or transmit FTI. Based on the inspection, corrective actions may be required in cases where the Contractor is found to be noncompliant with FTI safeguard requirements.

COMPLIANCE WITH HIPAA (HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996), HI-TECH (HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT OF 2009), AND OTHER HEALTH INFORMATION PRIVACY AND SECURITY LAWS

Definitions:
The following terms used in this Section shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information (PHI), Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

(a) Business Associate. "Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, and in this Section may refer to Contractor or its Subcontractor(s), to the extent Contractor or its Subcontractor(s) create, receive, maintain, or transmit protected health information on behalf of ITS.

(b) Covered Entity. By entering into the Contract, ITS does not affirm that it necessarily meets the definition of a "Covered Entity" or a "Business Associate" under the HIPAA statute, and rather affirms that ITS may in a given instance be acting as a "conduit" or in another capacity providing services to other entities, some of which themselves may be covered entities. But to the extent ITS is deemed to be covered by HIPAA or HI-TECH, the Parties agree the term "Covered Entity" in this Section shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103.

(c) HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

(d) "Medicaid Confidential Data" (MCD) includes all information about a Medicaid recipient or applicant, including enrollment information, eligibility data and protected health information. The NYS Department of Health (DOH) is the Single State Agency responsible for the administration of the New York State Medicaid program in New York State, including ensuring the security and confidentiality of MCD data.

HIPAA Protected Health Information Obligations and Activities of Contractor

To the extent Contractor or its Subcontractor(s) create, receive, maintain, or transmit protected health information on behalf of ITS pursuant to their responsibilities under the Contract, Contractor agrees that it is subject to, will abide by, and will require in writing its Subcontractors to similarly abide by, the following requirements applicable to Business Associates under HIPAA, agreeing to:

(a) Not use or disclose protected health information other than as permitted or required by the Contract or as required by law.

(b) Use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Contract.

(c) Report to ITS within ten (10) business days or fewer any use or disclosure of protected health information not provided for by the Contract of which it becomes aware. In no event shall Contractor exceed the timeframe for reporting to ITS breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware. Contractor shall provide ITS all information reasonably requested by ITS concerning any breach. Contractor shall also provide the following information to ITS upon first instance of the notification of breach: the identification of each individual whose unsecured protected health information has been, or is reasonably believed by Contractor, to have been, accessed, acquired, used, or disclosed during the breach.

(d) In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any Subcontractors that create, receive, maintain, or transmit protected health information on behalf of Contractor agree in writing to the same restrictions, conditions, and requirements that apply to Contractor with respect to such information.

(e) Make available protected health information in a designated record set to ITS, in a manner to be prescribed by ITS within a reasonable timeframe not to exceed fifteen (15) days, absent extenuating circumstances, as necessary to satisfy obligations which ITS or the entities it provides services to reasonably believe applicable to them under 45 CFR 164.524. In the event Contractor or its Subcontractor(s) receive any request for such protected health information directly from an individual, Contractor shall refer such request to ITS within a reasonable timeframe not to exceed ten (10) business days.

(f) Make any amendment(s) to protected health information in a designated record set as directed by ITS pursuant to 45 CFR 164.526 or take other measures as necessary to satisfy obligations that ITS reasonably believes it has under 45 CFR 164.526, in the manner as prescribed by ITS and within twenty (20) business days of such request. In the event Contractor or its Subcontractor(s) receive any request to amend a data set directly from an individual, Contractor shall refer such request to ITS within a reasonable timeframe not to exceed ten (10) business days.

(g) Maintain and make available the information required to provide an accounting of disclosures to ITS as necessary to satisfy obligations that ITS reasonably believes it has under 45 CFR 164.528, in the manner as prescribed by ITS and within ten (10) business days of such request. In the event Contractor or its Subcontractor(s) receive any request for an accounting of disclosures directly from an individual, Contractor shall refer such request to ITS within a reasonable timeframe not to exceed ten (10) business days.

(h) To the extent Contractor or its Subcontractor(s) are to carry out one or more of obligation(s) ITS may have under Subpart E of 45 CFR Part 164, in performing such obligations, comply with the requirements of Subpart E that apply to ITS; and

(i) Make either Contractor's or its Subcontractor(s)', or both's, internal practices, books, and records available to the Secretary of the Department of Health and Human Services and to ITS, for purposes of determining compliance with the HIPAA and HI-TECH Rules.

Permitted Uses and Disclosures of Protected Health Information by Contractor and its Subcontractor(s)

(a) Contractor and its Subcontractor(s) may only use or disclose protected health information as necessary to perform the services set forth in the Contract, provided however, that if de-identified information can be used in lieu of individually identifiable health information with the same effect, Contractor and its Subcontractor(s) shall use de-identified information in their performance of the Contract in accordance with 45 CFR 164.514(a)-(c).

(b) Contractor and its Subcontractor(s) may use or disclose protected health information as required by law.

(c) Contractor and its Subcontractor(s) agrees to make only those uses, disclosures and requests for protected health information that are consistent with the minimum necessary policies and procedures of ITS or the entit(ies) for whom ITS provides services which entail the creation, reception, maintenance, or transmittal of protected health information.

(d) Contractor and its Subcontractor(s) may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 except as may be provided for in the Contract or for the proper management and administration of Contractor or its Subcontractor(s), including the carrying out of the Contractor's or its Subcontractor(s)' legal responsibilities.

Other Health Information Obligations and Activities of Contractor

Contractor or its Subcontractor(s) may not disclose other types of health information protected by federal, State, or local law including but not limited to personally identifiable mental health information protected under NYS Mental Hygiene Law §33.16, other personally identifiable health information or HIV information protected under NYS Health Law sections §18 or Article 27-F, or substance abuse information protected under federal regulations 42 CFR Part 2.

Contractor or its Subcontractor(s) may not disclose Medicaid Confidential Data without the prior written approval of the New York State Department of Health (DOH), either directly or as provided to Contractor or its Subcontractor(s) through ITS. If contacted by DOH, while also informing ITS, Contractor or its Subcontractor(s) shall reasonably work with DOH to identify any individuals who may have inappropriately or unlawfully accessed Medicaid Confidential Data.

Contractor agrees to ensure that Contractor and any agent, including a Subcontractor, to whom Contractor provides Medicaid Confidential Data, agrees to the same restrictions and conditions that apply throughout the Contract. Further, Contractor agrees to state in any such agreement, contract, or document that the party to whom Contractor is providing the Medicaid Confidential Data may not further disclose it without the prior written approval of the New York State Department of Health. Contractor agrees to include the notices preceding, as well as references to statutory and regulatory citations set forth above, in any agreement, contract or document that Contractor enters into that involves Medicaid Confidential Data.

The federal Center for Medicare and Medicaid Services (CMS) requires that all contracts and/or agreements executed between the Department of Health and any second party that will receive Medicaid Confidential Data must include contract language that will bind such Parties to ensure that contractor(s) abide by the regulations and laws that govern the protection of individual, Medicaid confidential level data.

Medicaid Confidential Data includes all information about a recipient or applicant, including enrollment information, eligibility data and protected health information.

Contractor must comply with the following State and federal laws and regulations:

- Section 367b(4) of the NY Social Services Law
- New York State Social Services Law Section 369 (4)
- NYS Mental Hygiene Law §33.16,
- Article 27-F of the New York Public Health Law & 18 NYCRR 360-8.1
- Social Security Act, 42 USC 1396a (a)(7)
- Federal regulations at 42 CFR 431.302, 42 C.F.R. Part 2
- The Health Insurance Portability and Accountability act (HIPAA), at 45 CFR Parts 160 and 164

Please note that Medicaid Confidential Data released to Contractor may contain AIDS/HIV related NYS Confidential Information as defined in Section 2780(7) of the New York Public Health Law. As required by New York Public Health Law Section 2782(5), the following notice is provided to Contractor:

"This information has been disclosed to you from confidential records which are protected by state law. State law prohibits you from making any further disclosure of this information without the specific written consent of the person to whom it pertains, or as otherwise permitted by law. Any unauthorized further disclosure in violation of state law may result in a fine or jail sentence or both. A general authorization for the release of medical or other information is NOT sufficient authorization for the release for further disclosure."

Alcohol and Substance Abuse Related Confidentiality Restrictions:

Alcohol and substance abuse information is confidential pursuant to 42 C.F.R. Part 2. General authorizations are ineffective to obtain the release of such data. The federal regulations provide for a specific release for such data.

Term and Termination

(a) Termination for cause under HIPAA or HI-TECH. The Term of this Section shall be as described elsewhere in the "Term" section of the Contract. Among the other reasons for which ITS may terminate the Contract prior to the end of its Term date for cause, ITS may terminate the Contract if ITS determines the Contractor or its Subcontractor(s) have violated a material term of this HIPAA and HI-TECH Compliance Section of the Contract, and Contractor or its Subcontractor(s) have not cured the breach or ended the violation within any time that has been specified by ITS.

(b) Contractor's and its Subcontractor(s)' Obligations Upon Termination. Upon termination of the Contract for any reason, Contractor and its Subcontractor(s) shall return to ITS, transfer to another of ITS' contractors as directed by ITS, or, if agreed to by ITS on an individual case-by-case basis, destroy all protected health information received from ITS, or created, maintained, or received by the Contractor and its Subcontractor(s) on behalf of ITS, that the Contractor and its Subcontractor(s) still maintain in any form. Contractor and its Subcontractor(s) shall retain no copies of the protected health information. Contractor understands and agrees and will require of its Subcontractor(s) in writing that Contractor and its Subcontractor(s) are required to receive written approval from ITS prior to the return, transfer, or destruction of any protected health information.

(c) Survival. Contractor's and its Subcontractor(s)' obligations under this HIPAA and HI-TECH Compliance section of the Contract shall survive the termination of the Contract.

Miscellaneous

(a) Regulatory References. A reference in the Contract to a section in the HIPAA or HI-TECH Rules means the section as in effect or as amended.

(b) Amendment. The Parties agree to take such action as is necessary to amend the Contract from time to time as is necessary for compliance with the requirements of the HIPAA or HI-TECH Rules and any other applicable law.

(c) Interpretation. Any ambiguity in the Contract shall be interpreted to permit compliance with the HIPAA or HI-TECH Rules.

(d) Sub-contractors. Contractor shall require any Subcontractors that it uses that create, receive, maintain, or transmit protected health information on behalf of ITS under the Contract to conform to these HIPAA and HI-TECH Compliance requirements in addition to any other security, privacy, or applicable terms of the Contract.

D. QUESTIONS

All questions shall be emailed to the Designated Contact E-Mail Address indicated on the Cover Page of this RFQ.

Contractors are strongly encouraged to submit questions as early as possible. However, all questions must be submitted by the Question due date and time listed on the Cover Page of this RFQ. Answers to all questions of a substantive nature shall be provided to all Contractors who received this RFQ in the form of a question-and-answer document.

All Bids must conform to the terms set forth in this RFQ and the OGS Information Technology Umbrella Contract – Manufacturer Based. Extraneous terms or material deviations (including additional, inconsistent, conflicting, or alternative terms) may render the Bid non-responsive and may result in rejection of the Bid. Extraneous terms submitted on standard, pre-printed forms (including but not limited to product literature, order forms, license agreements, contracts, or other documents) that are attached or referenced with submissions shall not be considered part of the Bid or Authorized User Agreement but shall be deemed included for informational or promotional purposes only.

Each proposed extraneous term must be specifically enumerated in writing and specify the section of this RFQ that Bidder proposes to modify and the reasons why. Any extraneous terms must be submitted during the Question-and-Answer period as listed on the Cover Page of this RFQ. Extraneous terms submitted after this time will not be considered.

No extraneous term shall be incorporated into the Authorized User Agreement unless expressly accepted by ITS in writing. Acceptance and/or processing of a Bid shall not constitute acceptance of extraneous terms.

E. DOWNSTREAM PROHIBITION

None.

F. AUTHORIZED USER DISPUTE RESOLUTION PROCESS

Should a dispute or protest arise regarding this RFQ, the dispute or protest will be considered and decided by the Authorized User.

1. Disputes or Controversies Occurring During the Term of the Authorized User Agreement.
In the event there is a dispute or controversy during the term of the Authorized User Agreement resulting from this RFQ, the Contractor and Authorized User agree to exercise their best efforts to resolve the dispute as soon as possible. The Contractor and Authorized User shall, without delay, continue to perform their respective obligations under the resulting Authorized User Agreement and this Centralized Contract which are not affected by the dispute. Primary responsibility for resolving any dispute arising under the Authorized User Agreement shall rest with the persons designated by the Authorized User and the Contract's Contract Administrator and/or Account Manager.

In the event the Authorized User is dissatisfied with the Contractor's Products provided under the Authorized User Agreement, the Authorized User shall notify the Contractor in writing pursuant to the terms of the Contract. In the event the Contractor has any disputes with the Authorized User, the Contractor shall so notify the Authorized User in writing. If either party notifies the other of such dispute or controversy, the other party shall then make good faith efforts to solve the problem or settle the dispute amicably, including meeting with the party's representatives to attempt diligently to reach a satisfactory result.

If negotiation between such persons fails to resolve any such dispute to the satisfaction of the parties within fourteen (14) business days or as otherwise agreed to by the Contractor and Authorized User, of such notice, then the matter shall be submitted to the persons designated by the Authorized User and the Contractor's senior officer of the rank of Vice President or higher as its representative. Such representatives shall meet in person and shall attempt in good faith to resolve the dispute within the next fourteen (14) business days or as otherwise agreed to by the parties. This meeting must be held before either party may seek any other method of dispute resolution, including judicial or governmental resolutions. Notwithstanding the foregoing, nothing in this section shall be construed to prevent either party from seeking and obtaining temporary equitable remedies, including injunctive relief.

The Contractor shall extend the dispute resolution period for so long as the Authorized User continues to make reasonable efforts to cure the breach, except with respect to disputes about the breach of payment of fees or infringement of its or its licensors' intellectual property rights.

G. RESERVED RIGHTS

Bidders are hereby notified that New York State reserves the right to:

1. Reject any or all Bids received in response to the solicitation.
2. Withdraw the solicitation at any time, at the Agency's sole discretion.
3. Make an award under the solicitation in whole or in part.
4. Disqualify any Bidder whose conduct and/or Bid fails to conform to the requirements of the solicitation.
5. Seek clarifications and revisions of Bids.
6. Prior to the Bid deadline, amend the solicitation requirements to correct errors or oversights, or to supply additional information, as it becomes available.
7. Prior to the Bid deadline, direct Bidders to submit Bid modifications addressing subsequent solicitation amendments.
8. Change any of the schedule dates with timely notification to all prospective Bidders.
9. Eliminate any mandatory, non-material specifications that cannot be complied with by all of the prospective Bidders.
10. Waive any requirements that are not material.
11. Utilize any and all ideas submitted in the Bids received.
12. Negotiate with the Bidder responding to the solicitation within the solicitation requirements to serve the best interests of the State. This includes requesting increased discounts and clarifications of any or all Bidder's' Bids.
13. Require clarification at any time during the procurement process and/or require correction of arithmetic or other apparent errors for the purpose of assuring a full and complete understanding of a Bidder's Bid and/or to determine a Bidder's compliance with the requirements of the solicitation; and
14. Select and award to other than the selected Bidder(s) in the event of unsuccessful negotiations or, optionally, in other specified circumstances as detailed in the solicitation requirements.

15. Purchase none, some, all or more of the quantities of the items listed in Attachment 1 under this RFQ.
16. If applicable, consultants will be required to comply with ITS policies and procedures; pass background checks; and sign non-disclosure agreements.
17. If applicable, vendors may be required to complete Form A – Consultant Disclosure Form.
18. Extend the term of this agreement in accordance with the above outlined solicitation.

Manufacturer / Authorized Reseller Information

This Page is to be Completed By the Manufacturer or Authorized Reseller Responding to the RFQ		
The RFQ Response must be fully and properly executed by an authorized person. By signing you certify your express authority to sign on behalf of yourself, your company, or other entity and full knowledge and acceptance of this RFQ (including any Questions/Answers or addenda), the OGS Centralized Contract and that all information provided is complete, true and accurate. Quotes received by RFQ due date/time are binding and non-retractable for 120 days or as stipulated in the RFQ.		
Contract #	**Manufacturer Name**	**Authorized Reseller Name**
Manufacturer or Reseller Signature: *Date:*		*Phone Number:* *E-Mail:*
Printed or Typed Name:		*Title:*
If you are not providing a RFQ Response, place an "x" in the box, please explain why you are not responding, and return this page only. ☐ WE ARE UNABLE TO RESPOND AT THIS TIME BECAUSE:		

After fully completing the information above, please submit this page via e-mail with "Request for Quote – Financial Response – Cloud Solution" (Excel) to the Authorized User indicated on the Cover Page. Authorized User reserves the right to request the original executed page of this RFQ.

Request for Quote - Financial Response - Cloud Solution

RFQ Number	Authorized User Name	Contract Number	Manufacturer / Reseller Name	Date Completed	Grand Total
ITS-2024-526DB-Google Cloud SA	Information Technology Services (ITS)	PM67982			$52,323,067.84

Unanticipated Enhancements to Services is only applicable to items in Lot 4 - Implementation Services and is calculated based on the percentage the Authorized User chooses in cell E7 (not to exceed 20%).

Unanticipated Enhancements to Services (Not to Exceed 20%)	Implementation Base Total (*without* Unanticipated Enhancements)	Implementation Total (*with* Unanticipated Enhancements)	Recurring Cost Total	Data Transfer Cost Total
0%	$0.00	$0.00	$52,323,067.84	$0.00

Please See Request for Quotes for all Authorized User requirements.

Lot this RFQ Applies to: ☐ Lot 1 Software ☐ Lot 2 Hardware ☑ Lot 3 Cloud ☐ Lot 4 Implementation

If the RFQ includes Lot 4 – Implementation, Contractor must prior to submitting a response to the RFQ either hold an award for Lot 4- Implementation, or be able to provide the services under the other Lots included in the RFQ.

Instructions for When SKU's Have Been Identified by Authorized User

Authorized User will complete RFQ Number, Authorized User Name, Unanticipated Enhancements to Services Percent, Deliverable Number, Deliverable Name, Lot Number, Product Description(s), Manufacturer Part Number(s) (SKU), Net NYS Contract Price(s) and Qty, and Data Transfer Specifications in each of the three sections: Implementation Items, Recurring Items, and Data Transfer Items. The totals of each of these three sections will calculate into the Total Deliverable Cost. Please note, any anticipated deliverable travel costs are only applicable to items in Lot 4 - Implementation Services.
Manufacturer / Reseller will complete Deliverable Narrative, Additional Product Discount (Percentage), and optional Additional Product Discount (Dollars).

Instructions for When Authorized User Requires Vendor to Provide Suggested SKU's

Authorized User will complete RFQ Number and Authorized User Name, Unanticipated Enhancements to Services Percent, and Data Transfer Specifications in each of the three sections: Implementation Items, Recurring Items, and Data Transfer Items. The totals of each of these three sections will calculate into the Total Deliverable Cost. Please note, any anticipated deliverable travel costs are only applicable to items in Lot 4 - Implementation Services.
Manufacturer / Reseller will complete Deliverable Number, Deliverable Name, Deliverable Narrative, Lot Number, Product Description, Manufacturer Part Number (SKU), Net NYS Contract Price, Additional Product Discount (Percentage), Qty and optional Additional Product Discount (Dollars) to meet a defined need as detailed in the Authorized User Request for Quote.

Deliverable Information

Deliverable Number	Deliverable Name

Implementation Items

RFQ Item Number	Lot Number	Product Description	Manufacturer Part Number (SKU)	Net NYS Contract Price	Additional Product Discount (Percentage)	RFQ Product Price	Qty	Additional Product Discount (Dollars)	Extended RFQ Price	Unanticipated Enhancements to Services (Not to Exceed 20%)
1										
2										
3										
4										
5										
								Anticipated Deliverable Travel Costs (Lot 4 - Implementation Services only)		$0.00
								Total Deliverable Implementation Cost	$0.00	$0.00

RFQ Number	Authorized User Name	Contract Number	Manufacturer / Reseller Name	Date Completed	Grand Total
ITS-2024-526DB-Google Cloud SA	Information Technology Services (ITS)	PM67982			$52,323,067.84

Unanticipated Enhancements to Services is only applicable to items in Lot 4 - Implementation Services and is calculated based on the percentage the Authorized User chooses in cell E7 (not to exceed 20%).

Unanticipated Enhancements to Services (Not to Exceed 20%)	Implementation Base Total (*without* Unanticipated Enhancements)	Implementation Total (*with* Unanticipated Enhancements)	Recurring Cost Total	Data Transfer Cost Total
0%	$0.00	$0.00	$52,323,067.84	$0.00

Please See Request for Quotes for all Authorized User requirements.

Recurring Items

RFQ Item Number	Lot Number	Product Description	Manufacturer Part Number (SKU)	Net NYS Contract Price	Additional Product Discount (Percentage)	RFQ Product Price	Qty	Additional Product Discount (Dollars)	Extended RFQ Price
		Year One - Term Dates to be determined							
1	Lot 3	[redacted]		$0.99		$0.99	[redacted]		
2	Lot 3			$0.99		$0.99			
3	Lot 3			$4.51		$4.51			
4	Lot 3			$5.88		$5.88			
5	Lot 3			$14,700.00		$14,700.00			
6	Lot 3			$12,250.00		$12,250.00			
7	Lot 3			$0.99		$0.99			
8	Lot 3			$0.99		$0.99			
9	Lot 3			$4.51		$4.51			
10	Lot 3			$5.88		$5.88			
11	Lot 3			$14,700.00		$14,700.00			
12	Lot 3			$12,250.00		$12,250.00			
13									
14									
15									
							Total Deliverable Recurring Cost		$52,323,067.84

RFQ Number	Authorized User Name	Contract Number	Manufacturer / Reseller Name	Date Completed	Grand Total
ITS-2024-526DB-Google Cloud SA	Information Technology Services (ITS)	PM67982			$52,323,067.84

Unanticipated Enhancements to Services is only applicable to items in Lot 4 - Implementation Services and is calculated based on the percentage the Authorized User chooses in cell E7 (not to exceed 20%).

Unanticipated Enhancements to Services (Not to Exceed 20%)	Implementation Base Total (*without* Unanticipated Enhancements)	Implementation Total (*with* Unanticipated Enhancements)	Recurring Cost Total	Data Transfer Cost Total
0%	$0.00	$0.00	$52,323,067.84	$0.00

Please See Request for Quotes for all Authorized User requirements.

Data Transfer Items

Data Transfer Specifications:

RFQ Item Number	Lot Number	Product Description	Manufacturer Part Number (SKU)	Net NYS Contract Price	Additional Product Discount (Percentage)	RFQ Product Price	Qty	Additional Product Discount (Dollars)	Extended RFQ Price	Unanticipated Enhancements to Services (Not to Exceed 20%)
1										
2										
3										
4										
5										
								Anticipated Deliverable Travel Costs (Lot 4 - Implementation Services only)		
								Total Deliverable Data Transfer Cost	$0.00	$0.00

Total Deliverable Cost	$52,323,067.84