HHS reserves the right to exercise priorities and allocations authority with respect to this contract, to include rating this order in accordance with 45 CFR Part 101, Subpart A— Health Resources Priorities and Allocations System.

SECTION 1 – SUPPLIES OR SERVICES/PRICES

1.1 DESCRIPTION/SPECIFICATIONS/ TITLE:

The purpose of this PWS is to outline proposed Contractor support to assist the HHS Office of the Chief Information Officer (OCIO) with leveraging wastewater data to detect trends in COVID-19 cases in the community and including that data in the HHS Protect Program.

1.2 DESCRIPTION/PERFORMANCE WORK STATEMENT

Under the direction of the White House Coronavirus Task Force, the Department of Health and Human Services (HHS) and our federal partners are working with state, local, tribal and territorial governments and with the private sector to execute a whole of government response to fight the COVID-19 pandemic and protect the public's health.

To that end, Departmental leadership and HHS Operating and Staff Divisions are working to obtain sufficient and necessary data to address the needs of this public health emergency. Through the authorities under the Foundations for Evidence-Based Policymaking Act, the HHS CIO/CDO is responsible for ensuring the effective execution of data management practices across our organization. Data collection and analysis is of the utmost importance in responding to COVID-19 and coordinating efforts to collect that data will accelerate our work to protect the public and lessen the spread and impact of this virus. With the increasing number of cases in the United States and across the globe, it is critical for the United States Government to have access to all available resources to support efforts in the response.

This requirement is a critical and urgently need to support the nation's response to the COVID-19 health emergency. The HHS Protect platform is critical to manage data and information for HHS to the nation, White House task force, and the National Response Coordination Center. The HHS OCIO has a requirement to immediately provide this capability to the various senior decision makers that are providing medical and pharmaceutical related material and services to various locations across the US during this public health emergency.

This HHS Data Sharing platform is critical to the COVID-19 White House Task Force, the HHS response teams, and the inter-governmental COVID-19 teams that are hosted by the FEMA National Response and Coordination Center. In furtherance of this need, we are planning to ingest HHS data sets on the HHS COVID-19 Data Sharing Platform, as well as, publicly available data sets, state and local data sets, and private sector data sets. These data are the foundation for the White House's decision-making and daily public presentations.

These data sets may contain certain sensitive data elements, including residual personally identifiable information that are required in furtherance of these COVID-19 response efforts therefore data protection is critical. We will be integrating multiple products to address issues related to role-based access – what levels of data are needed, how to accomplish secure data transmission, and to ensure awareness of the anticipated level of use and sharing of data provided.

Trends in SARS-CoV-2 concentrations in wastewater have been demonstrated to correlate with trends in new COVID-19 cases 5 to 11 days in the future. Wastewater testing data provided by the Contractor will illustrate a more complete picture of local, community-level COVID-19 trends, where clinical cases may be underreported and transmission levels not well understood. This can be particularly helpful for communities with limited testing

access, or for communities in which demand for testing remains low for other reasons. The Contractor will work with HHS to find the best path forward so that testing can have the greatest impact on the overall health of the American populace.

Scope:

The Contractor shall provide additive data and support to the HHS Protect Program by detecting pathogen SARS-CoV-2 in community wastewater, compiling that data, performing predictive analysis on that data, and securely transferring the derived data into the HHS Protect system in a JSON format that corresponds with the Federal Information Processing Standard Publication (FIPS) code level. The contractor shall support wide-scale and regular testing of the American population for COVID-19 using wastewater surveillance to help guide reopening and mitigation strategies, and also serve as leading indicator for local re-emergence events to enable rapid containment.

As set forth below, Contractor, at the direction of HHS/OCIO, shall go to Authorized Communities, and perform the services listed below in this section. An Authorized Community is defined as a city, town, or other locality for which HHS/OCIO has directed a Contractor to provide wastewater surveillance testing services for SARS-CoV-2 with appropriate quality assurance and quality controls. HHS/OCIO shall provide direction to Contractor regarding the Authorized Community, frequency of testing, and approved number of sample collection locations. Contractor may reject the assignment of an Authorized Community, provided that in order to do so Contractor must notify HHS/OCIO in writing within 48 hours of being assigned an Authorized Community that it rejects this assignment.

The Contractor must provide all staff, equipment, supplies, and logistical support to perform all services described in this contract, including but not limited to, identification of sample collection location, sample collection, and sample analysis. This will include supplying sample collection equipment. This Performance Work Statement (PWS) addresses these areas for the performance of this work:

1. Program management,
2. Engagement in a documented planning process,
3. Collection of wastewater samples from approved sample collection locations on a regular basis in Authorized Communities as established in consultation with HHS;
4. Analysis and provision of SARS-CoV-2 RNA concentration data and associated metadata from wastewater treatment plants for predictive analysis
5. Rapid, secure data file transfers to HHS Protect

Leveraging wastewater data to predict new COVID-19 cases

The contractor shall support wide-scale and regular testing of the American population for COVID-19 using wastewater epidemiology to help guide the overall reopening strategy, but also serve as an early warning system for local re-emergence events to enable rapid containment.

The contractor shall work with communities across 42 states and establish COVID-19 wastewater testing for over 10% of the American population. They will scale these testing regimes as they will serve as an invaluable early warning system to guide local and national strategies controlling the spread of the COVID-19 outbreak.

A national wastewater testing platform for HHS

The contractor shall scale COVID-19 wastewater testing, in phases, in the United States. This network will generate qualitative trend data of SARS-CoV-2 concentrations in sewage, providing critical information on how to strategically reopen American cities and the economy, and an early warning for new outbreaks.

Wastewater testing is predictive of new COVID-19 cases 5 to 11 days in advance. Data and analysis provided by the contractor's wastewater surveillance will illustrate a more complete picture of local, community level COVID-19 trends, where clinical cases had been dangerously underreported, leading to unchecked spread. This can be particularly helpful for communities lacking testing facilities or testing supplies, or for communities in which demand for testing remains low for other reasons.

Clinical testing lags 5-11 days behind wastewater surveillance, giving public officials a planning advantage and enabling an adequate operational response. The contractor will work with HHS to find the best path forward so that testing can have the greatest impact on the overall health of the American populace.

Data Use

All wastewater samples collected through this contract, along with their associated data and reporting, or any other derivative information the Contractor uses, maintains, discloses, receives, creates, transmits or otherwise obtains in connection with its performance of the Project, are the sole property of HHS. Under no circumstances may Contractor use these samples, or any data generated with, by, or from these samples, for purposes not explicitly described in this Contract or without prior written approval from HHS. Examples of prohibited uses include, but are not limited to, testing of wastewater samples collected pursuant to this Contract other than as provided for in this Contract, inclusion in research publications, data sharing with other public or private entities, or incorporation into marketing materials.

The Contractor shall report to HHS, both verbally and in writing, any instance in which a sample or any other data obtained in connection with this contract is subpoenaed or becomes the subject of a court or administrative order or other legal process (including a public records request under the Freedom of Information Act). The Contractor shall provide such report to HHS as soon as feasible upon receiving or otherwise becoming aware of the legal process; provided, that the Contractor shall provide such report no later than five (5) business days prior to the applicable response date. If HHS determines that it shall respond directly, the Contractor shall cooperate and assist HHS in its response.

The Contractor shall implement administrative, physical and technical safeguards that reasonably and appropriately protect the samples and that prevent use or disclosure of such data other than as provided for by this Contract. As soon as possible, but in any event no later than twenty-four (24) hours after Contractor becomes aware of a misuse or mis-disclosure not permitted under the Contract, the Contractor shall verbally report the Event to HHS with as much of the details listed below as possible, and shall follow such verbal report within three (3) business days with a written report outlining the misuse or mis-disclosure and shall provide any additional information as HHS may reasonably request. The Contractor acknowledges that samples subject to this contract are sensitive, and violations of this section shall be deemed a material breach of the Contract.

Tasks

Phase 0: Rapid ramp-up of testing deployment and establishment of data transfer protocols between Contractor and HHS Protect.

Period of performance, 2 weeks

1. Establish and test data transfer protocols between Contractor and HHS Protect
2. Leverage existing and prior contractor relationships with wastewater treatment plants to ramp-up and onboard testing to cover ~36 million people, ~ 100 wastewater treatment plants, ~10% of the population.

Deliverables

- Contractor shall establish and test secure data transfer to HHS Protect
- Contractor shall prepare and host at least two training sessions, no less than 30 minutes/each, for the government and their representatives, covering how to digest and analyze the provided data
- Contractor shall provide data collection instrument for required wastewater treatment plant metadata.
- Contractor shall provide thorough documentation and guides for HHS to analyze the data streams

Phase 1: Testing and reporting for~36 million people, ~100 wastewater treatment plants, ~ 10% of the US population including quality assurance and quality control (QA/QC)

Period of Performance: 6 weeks

1. Contractor will provide self-contained sampling kits to participating wastewater facilities for 24-hour composite samples (if capacity available at wastewater facility), or grab samples, greater than or equal to 500 ml.
2. Provide training to wastewater facility staff on proper collection, packaging, and shipping of composite sample of their wastewater, safely packaging and returning to the contractor. Sample collection and shipping protocols are provided.
3. Contractor runs laboratory analysis, isolating the genetic material (RNA) of SARS-CoV-2 and analyzing and testing to quantify the amount of SARS-CoV-2 RNA molecular targets via reverse transcriptase quantitative polymerase chain reaction or droplet digital RT-PCR.
4. Contractor uses computational biology models to identify strains circulating in the state, and to estimate COVID-19 cases.
5. Contractor expedites reporting, contextualizing data with thousands of samples collected across 42 states to date.
6. Contractor performs QA/QC controls to maintain the uncorrupted nature of the raw and modeled data required, including but not limited to, protocol of laboratory methods utilized, human fecal normalization parameter, inhibition evaluation, standard curves (RT-qPCR), extraction blanks, and no template controls.
7. Contractor provides regular data streams to HHS Protect, at a minimum of 2x/week.

Deliverables

- Transfer derived data to HHS a minimum of 2x/week.
- Report testing performance including QA/QC, turnaround time, and percent of samples requiring repeat testing.
- One additional 30-minute training sessions with the government and their representatives;

Task 2: Target expansion to ~100 million people, ~320 wastewater treatment plants, ~30% of the US population

Optional: (must be exercised by the government),

Period of Performance: 9 weeks

Task 2 includes all the steps outlined in Task 1, but at an expanded footprint of sample collection sites to approximately 350 wastewater treatment plants covering approximately 30% of the US population, which the Contractor will coordinate with HHS to identify.

Note: Task 2 is contingent on the successful completion of Task 1. The government will determine the value of a continued data transfer from the contractor to HHS Protect.

Task 3: Contractor Program Management

The Contractor shall manage their performance to ensure compliance with all requirements of the contract. The Contractor shall assign a Program Manager who will ensure the Contractor's performance complies with all requirements and will be the primary point of contact for the work to be performed. The Program Manager shall have sufficient corporate authority to direct, execute, and control all elements of the task and ensure that all necessary management, business, contracts, engineering, implementation, and maintenance resources are available and sufficient, both in numbers and qualifications, to successfully perform all the tasks required by the contract.

The Contractor shall continuously monitor the performance of this contract, and of all subcontracts, to provide the Government with a timely assessment of program progress and problems and to control contract activities to include Subcontractor and/or vendor activities. This should involve the development and execution of a Communication Plan to include the methodology and approach for communicating status, issues, and risks to OCIO through the COR and for communicating with stakeholders outside OCIO. Critical management data regarding OCIO operations status and high priority projects should be available on an electronic Dashboard.

Deliverables:

- Kick off Meeting
- Status Report (Weekly)
- Monthly Contract Review Meetings (Frequency: Monthly)

Performance Standards:

Task Description	Performance Indicator	Required Performance Measurement
Providing data transfers into HHS Protect	Delivery Time	Data transfer is completed – without delays or errors – 2x/week
Providing consistently complete data	Accuracy	Deliverables require two revisions or less
HHS Protect Support	Response Time	Respond to all inquiries & requests for assistance within one business day

MINIMUM REQUIREMENTS

Contractor certifies that it meets the following minimum requirements for entering into the Contract:

1. Contractor has the capacity to perform wastewater testing for SARS-CoV-2 and associated Quality Assurance/Quality Control (QA/QC) required for on a maximum of 200 samples per week for 8 weeks in Phase 1 and up to 640 samples per week for 9 weeks in Phase 2 (optional).

2. Contractor can consistently report results of wastewater surveillance testing within 36 hours of sample collection for the duration of this Contract.

3. Contractor can specify appropriate QA/QC measures and document their implementation as a part of their wastewater analysis methodology.

4. Contractor has the demonstrated capacity to independently forge partnerships with local officials, including but not limited to local water/sewer departments.

5. Contractor has previous experience performing wastewater testing activities with appropriate QA/QC measures in the United States.

6. Contactor can secure all equipment necessary to perform the services required under this Contract.

7. Contractor has all appropriate licenses or waivers in place to perform all wastewater testing services.

1.3 TYPE OF CONTRACT

This is a Firm Fixed Price Task Order for severable, commercial items/services.

The services acquired under this contract are severable services. Funds are only available for use for the contract line item (CLIN) to which they are obligated. Unused funds from one CLIN may not rollover for use in other CLINs.

1.4 COMMERCIAL ITEMS

COMMERCIAL ITEMS/SERVICES:

The services specified in this task order have been determined to be commercial.

CONSIDERATION AND PAYMENT (Fixed Price – Severable Services)

Base: September 30, 2020 through November 25, 2020 (8 weeks)

Option Period One: November 26, 2020 through January 27, 2021 (9 weeks)

In consideration of satisfactory performance/delivery of the work as described throughout this contract, the Contractor shall be paid a fixed price for each CLIN. The contract is priced as follows:

CLIN	Item/Part Number	Description	QTY/WEEKS	Unit Price	Extended Price
1			8	$	$
2			9	$	$
TOTAL FFP					$

SECTION 2 – DELIVERIES OR PERFORMANCE

2.1 PERIOD OF PERFORMANCE

The period of performance shall be for a base period of twelve (12) months from the date of award, with anticipated award date of July 29, 2020, as follows:

Base Period: 09/30/2020 – 11/25/2020
Option Period One: 11/26/2020 – 01/27/2021

2.2 PLACE OF DELIVERY/PERFORMANCE

Work will be performed at the Contractor's site, but the contractor is not prohibited from allowing its employees to telework in accordance with the contractor's policies if the work and required level of performance can be completed successfully in accordance with the contract requirements. The Contractor shall coordinate employee telework or any on-site Government location delivery/support in advance with the Contracting Officer's Representative.

Delivery information is as follows:
Procurement Name: Wastewater Data Testing

Procurement POP: September 30, 2020 through November 25, 2020
Technical Point of Contact: TBD
POC Email: TBD
POC Telephone:
COR: TBD
COR Email: TBD
COR Telephone:
Delivery Address for Hardware/Software: Via email to COR and Technical POC; 200 Independence Avenue, Washington DC 20001

2.3 REPORTS/DELIVERABLES AND DELIVERY/PERFORMANCE SCHEDULE

The purpose of the effort is to assist HHS-OCIO migrate its legacy application portfolio to a standardized modern platform that provides ease of integration with other HHS-OCIO technology platforms. Reference deliverables listed in Scope and Tasks; deliverables include:

- Kick off Meeting
- Status Report (Weekly)
- Monthly Contract Review Meetings (Frequency: Monthly)

Contractor Performance Evaluation:

During the life of this TO, contractor performance will be evaluated on an interim and final basis pursuant to FAR Subpart 42.15. The Contractor Performance Assessment Reporting System (CPARS) will be utilized for these reviews. Information on CPARS can be located at http://www.cpars.gov.

QUALITY ASSURANCE SURVEILLANCE PLAN (QASP)

The Government intends to utilize the below Quality Assurance Surveillance Plan (QASP) to monitor the quality of the Contractor's performance. The oversight provided for in the contract and in the QASP will help to ensure that service levels reach and maintain the required levels throughout the contract term. Further, the QASP provides the COR with a proactive way to avoid unacceptable or deficient performance, and provides verifiable input for the Contractor Performance Assessment Reporting System (CPARS). The QASP may be updated by modification to the contract.

Quality Assurance Surveillance Plan (QASP)

Task	Standard	Acceptable Quality Limit
All deliverables	Deliverables are completed by the required due dates.	95% of deliverables

Task	Standard	Acceptable Quality Limit
	For each deliverable requiring government approval, less than 10 percent content rework is required.	100% of deliverables
	Upon resubmission reworked deliverables are compliant.	100% of reworked deliverables
Schedule management	Over the life of the program, milestone completion dates defined in the integrated master schedule and PMP change less than 10 percent from the PMO-approved baseline.	100% compliance
Standards	Design is compliant with statutory and regulatory standards, HHS policy, and federal enterprise architecture standards.	100%
Testing	All systems are tested and perform per approved design and system specifications.	95% pass rate
	Remediated defects pass UAT testing upon first resubmission and do not cause cascading defects.	98% of defects
	All show stopper defects must be resolved before scheduled release.	100% show stoppers
Implementation	Systems are given authority to operate prior to go live date.	100%
Collaboration	Contractor adheres to agreed upon standards of behavior and conduct.	100%
Transition Out/Knowledge Transfer	EA receives the referenced documentation and knowledge transfer to successfully operate and maintain Vision Application Portfolio Management and related interfaces post contract completion.	As evaluated by the EA Executive and PMO
Stabilization and user acceptance	During the stabilization period, Contractor is responsive and resources are applied to support acceptance and adoption of the system by the user community.	As evaluated by the EA PMO

2.3 NOTICE TO THE GOVERNMENT OF DELAYS

In the event the Contractor encounters difficulty in meeting performance requirements, or when the Contractor anticipates difficulty in complying with the contract delivery schedule or completion date, or whenever the Contractor has knowledge that any actual or potential situation is delaying or threatens to delay the timely performance of this contract, the Contractor shall immediately notify the Contracting

Officer, the Contracting Officer's Representative and the Program Management Office, in writing, giving pertinent details. This data shall be informational only in character and this provision shall not be construed as a waiver by the Government of any delivery schedule or date, or any rights or remedies provided by law or under this task order.

Performance Standards:

Task Description	Performance Indicator	Required Performance Measurement
Providing data transfers into HHS Protect	Delivery Time	Data transfer is completed – without delays or errors – 2x/week
Providing consistently complete data	Accuracy	Deliverables require two revisions or less
HHS Protect Support	Response Time	Respond to all inquiries & requests for assistance within one business day

SECTION 3 - Contract Administration Data

3.1 AUTHORITIES OF GOVERNMENT PERSONNEL

Notwithstanding the Contractor's responsibility for total management during the performance of this contract, the administration of this contract will require maximum coordination between the Government and the Contractor. The following individuals will be the Government's points of contact during the performance of this contract:

Contracting Officer
Name: Jennifer Browning
Email: jennifer.browning@hhs.gov

Contracting Officer's Representative
Name: TBD
Address: 200 Independence Ave, S.W., Washington DC 20201
Email: TBD

Note: The Contracting Officer is the only individual authorized to modify the contract.

3.2 CONTRACTING OFFICER'S REPRESENTATIVE (COR) AUTHORITY

(a) Performance of work under this contract must be subject to the technical direction of the Contracting Officer's Representative identified above, or a representative designated in writing. The term "technical direction" includes, without limitation, direction to the contractor that directs or redirects the labor

effort, shifts the work between work areas or locations, fills in details and otherwise serves to ensure that tasks outlined in the work statement are accomplished satisfactorily.

(b) Technical direction must be within the scope of the specification(s)/work statement.

The Contracting Officer's Representative does not have authority to issue technical direction that:

(1) Constitutes a change of assignment or additional work outside the specification(s)/statement of work;

(2) Constitutes a change as defined in the clause entitled "Changes";

(3) In any manner causes an increase or decrease in the contract price, or the time required for contract performance;

(4) Changes any of the terms, conditions, or specification(s)/work statement of the contract;

(5) Interferes with the contractor's right to perform under the terms and conditions of the contract; or

(6) Directs, supervises or otherwise controls the actions of the contractor's employees.

(c) Technical direction may be oral or in writing. The Contracting Officer's Representative shall confirm oral direction in writing within five work days, with a copy to the Contracting Officer.

(d) The contractor shall proceed promptly with performance resulting from the technical direction issued by the Contracting Officers, Representative. If, in the opinion of the contractor, any direction of the Contracting Officers, Representative, or his/her designee, falls within the limitations in (b), above, the contractor shall immediately notify the Contracting Officer no later than the beginning of the next Government work day.

(e) Failure of the contractor and the Contracting Officer to agree that technical direction is within the scope of the contract shall be subject to the terms of the clause entitled "Disputes."

3.3 INVOICE SUBMISSION

(1) Invoice Submission

The contractor shall submit invoices under this contract once per month. Invoices shall be submitted in accordance with the contract terms.

A proper invoice, with all required back-up documentation shall be sent electronically, via email, to:

1) Contracting Officer's Representative (COR): *TBD*
2) Contracting Officer: *Jennifer.browning@hhs.gov*
3) Contract Specialist: *Lashawn.Haggins@hhs.gov*
4) Financial Management Services: psc_invoices@psc.hhs.gov
5) Acquisition Management Services: pscsas.invoices@psc.hhs.gov

The subject line of the invoice submission email shall contain the contract number, order number (if applicable), and the number of invoices contained within. Each invoice shall be submitted as a single file, limited in size to 25MB, which includes all required back-up documentation based on the contract type. In the event an invoice file exceeds the size limitation, the contractor shall contact the Contracting Officer to provide all required supporting documentation. The email may have multiple invoices for the contract. Invoices must be in the following formats: PDF, TIFF, or Word. No Excel formats will be accepted. The electronic file cannot contain multiple invoices; example, 10 invoices requires 10 separate files.

(2) Invoice Elements

Invoices must include all elements required by FAR 52.212-4(g). The contractor is required to include electronic funds transfer (EFT) banking information. In accordance with the requirements of the Debt Collection Improvement Act of 1996, all payments under this contract will be made by electronic funds transfer (EFT). The Contractor shall provide financial institution information to the Finance Office designated above in accordance with FAR 52.232-33 Payment by Electronic Funds Transfer - System for Award Management.

Additionally, the Program Support Center (PSC) requires:

(i) Invoices must break-out price/cost by contract line item number (CLIN) as specified in the pricing section of the contract.

(ii) Invoices must include the Dun & Bradstreet Number (DUNS) of the Contractor.

(iii) Invoices that include time and materials or labor hours CLINS must include supporting documentation to (1) substantiate the number of labor hours invoiced for each labor category, and (2) substantiate material costs incurred (when applicable).

3) Prompt Payment Act

Invoices will be handled in accordance with the Prompt Payment Act (31 U.S.C. 3903) and Office of Management and Budget (OMB) prompt payment regulations at 5 CFR Part 1315.

SECTION 4 - Special Contract Requirements

4.1 PRIVACY AND SECURITY REQUIREMENTS

Contractor must comply with or receive an applicable waiver for all HHS-OCIO security, privacy, and section 508 requirements.

4.2 KEY PERSONNEL

The key personnel specified in this contract are considered to be essential to work performance. At least 30 days prior to the contractor voluntarily diverting any of the specified individuals to other programs or contracts the Contractor shall notify the Contracting Officer and shall submit a justification for the diversion or replacement and a request to replace the individual. The request must identify the proposed replacement and provide an explanation of how the replacement's skills, experience, and credentials meet or exceed the requirements of the contract (including, when applicable, Human Subjects Testing requirements). If the employee of the contractor is terminated for cause or separates from the contractor voluntarily with less than thirty days notice, the Contractor shall provide the maximum notice practicable under the circumstances. The Contractor shall not divert, replace, or announce any such change to key personnel without the written consent of the Contracting Officer. The Government does not currently identify any key personnel. The contract will be modified to add or delete key personnel as necessary to reflect the agreement of the parties.

4.3 HHS PRIVACY AND SECURITY REQUIREMENTS

Data Jurisdiction. The contractor shall store all information within the security authorization boundary, data at rest or data backup, within the continental United States (CONUS) if so required.

Service Level Agreements. The Contractor shall understand the terms of the service agreements that define the legal relationships between cloud customers and cloud providers and work with OPS to develop and maintain an SLA.

Interconnection Agreements/Memorandum of Agreements. The Contractor shall establish and maintain Interconnection Agreements and or Memorandum of Agreements/Understanding in accordance with HHS/OS policies.

4.4 REQUIREMENTS FOR CLOUD SERVICES

HHS Privacy and Security Requirements

The Contractor (and/or any subcontractor) shall be responsible for the following privacy and security requirements:

HHS Compliant ATO. As applicable, since Vision Data Sharing Platform relies upon an existing moderate HHS compliant solution – Oracle Federal Managed Cloud Services. The contractor shall comply with HHS Security Assessment and Authorization (SA&A) requirements and to ensure the information system/service under this contract maintains a valid HHS compliant (approved) authority to operate

(ATO) in accordance with Federal Information Processing Standard (FIPS) Publication 199 defined security categorization.

a) Implement applicable baseline controls commensurate with the agency-defined security categorization and the applicable security control baseline. The *HHS Information Security and Privacy Policy (IS2P)* a Outlines controls identified by the agency.

b) A security control assessment must be conducted by an HHS third-party assessment organization for the initial ATO and ***annually*** thereafter or whenever there is a significant change to the system's security posture in accordance with the application's Continuous Monitoring Plan.

1. **Data Jurisdiction.** The contractor shall store all information within the security authorization boundary, data at rest or data backup, within the continental United States (CONUS).
2. **Interconnection Agreements/Memorandum of Agreements.** The Contractor shall establish and maintain Interconnection Agreements and or Memorandum of Agreements/Understanding in accordance with HHS policies.

4.5 PROTECTION OF INFORMATION IN A CLOUD ENVIRONMENT

1) If contractor (and/or any subcontractor) personnel must remove any information from the primary work area, they shall Vision it to the same extent they would the proprietary data and/or company trade secrets and in accordance with HHS policies.
2) HHS will retain unrestricted rights to federal data handled under this contract. Specifically, HHS retains ownership of any user created/loaded data and applications collected, maintained, used, or operated on behalf of HHS and hosted on contractor's infrastructure, as well as maintains the right to request full copies of these at any time. If requested, data must be available to HHS within ***one (1) business day*** from request date or within the timeframe specified otherwise. In addition, the data shall be provided at no additional cost to HHS.
3) The Contractor (and/or any subcontractor) shall ensure that the facilities that house the network infrastructure are physically and logically secure in accordance with HHS requirements and policies.
4) The contractor shall support a system of records in accordance with NARA-approved records schedule(s) and protection requirements for federal agencies to manage their electronic records in accordance with 36 CFR § 1236.20 & 1236.22 (ref. a), including but not limited to the following:
   a. Maintenance of links between records and metadata, and
   b. Categorization of records to manage retention and disposal, either through transfer of permanent records to NARA or deletion of temporary records in accordance with NARA-approved retention schedules.
5) The disposition of all HHS data shall be at the written direction of HHS. This may include documents returned to HHS control; destroyed; or held as specified until otherwise directed. Items returned to the Government shall be hand carried or sent by certified mail to the COR.
6) If the system involves the design, development, or operation of a system of records on individuals, the Contractor shall comply with the Privacy Act requirements.

A. Security Assessment and Authorization (SA&A) Process

1) The Contractor (and/or any subcontractor) shall comply with HHS requirements as mandated by federal laws, regulations, and HHS policies, including making available any documentation, physical access, and logical access needed to support the SA&A

requirement. The level of effort for the SA&A is based on the system's FIPS 199 security categorization and HHS security policies.

a. The contractor shall complete and maintain an agency SA&A package to obtain agency ATO prior to system deployment/service implementation. The agency ATO must be approved by the HHS authorizing official (AO) prior to implementation of system and/or service being acquired.

2) HHS reserves the right to perform penetration testing (pen testing) on all systems operated on behalf of agency. If HHS exercises this right, the Contractor (and/or any subcontractor) shall allow HHS employees (and/or designated third parties) to conduct Security Assessment activities to include control reviews in accordance with HHS requirements. Review activities include, but are not limited to, scanning operating systems, web applications, wireless scanning; network device scanning to include routers, switches, and firewall, and IDS/IPS; databases and other applicable systems, including general support structure, that support the processing, transportation, storage, or security of Government information for vulnerabilities.
3) The Contractor must identify any gaps between required HHS Security Control Baseline/Continuous Monitoring controls and the contractor's implementation status as documented in the Security Assessment Report and related Continuous Monitoring artifacts. In addition, all gaps shall be documented and tracked by the contractor for mitigation in a Plan of Action and Milestones (POA&M) document. Depending on the severity of the risks, HHS may require remediation at the contractor's expense, before HHS issues an ATO.
4) The Contractor (and/or any subcontractor) shall mitigate security risks for which they are responsible, including those identified during SA&A and continuous monitoring activities. All vulnerabilities and other risk findings shall be remediated by the prescribed timelines from discovery: (1) critical vulnerabilities no later than ***thirty (30) days*** and (2) high, medium and low vulnerabilities no later ***than sixty (60) days.*** In the event of a vulnerability or other risk finding cannot be mitigated within the prescribed timelines above, they shall be added to the designated POA&M and mitigated within the newly designated timelines. HHS will determine the risk rating of vulnerabilities using HHS baselines.
5) **Revocation of a Cloud Service**. HHS has the right to take action in response to the CSP's lack of compliance and/or increased level of risk. In the event the CSP fails to meet HHS security and privacy requirements and/or there is an incident involving sensitive information, HHS and **may** suspend or revoke an existing agency ATO (either in part or in whole) and/or cease operations. If an ATO is suspended or revoked in accordance with this provision, the CO and/or COR may direct the CSP to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor information system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

B. Reporting and Continuous Monitoring

1) Following the initial ATOs, the CSP (and/or any subcontractor) must perform the minimum ongoing continuous monitoring activities specified below, submit required deliverables by the specified due dates, and meet with the system/service owner and other relevant

stakeholders to discuss the ongoing continuous monitoring activities, findings, and other relevant matters. The CSP will work with the agency to schedule ongoing continuous monitoring activities.

2) At a minimum, the CSP Contractor must provide the following artifacts/deliverables on a ***monthly*** basis

a. Operating system, database, Web application, and network vulnerability scan results;
b. Updated POA&Ms;
c. Any updated authorization package documentation as required by the annual attestation/assessment/review or as requested by the System Owner or AO; and
d. Any configuration changes to the system and/or system components or CSP's cloud environment that may impact HHS's security posture. Changes to the configuration of the system, its components, or environment that may impact the security posture of the system under this contract must be approved by the agency.

C. Configuration Baseline

1) The contractor and CSP shall certify that applications are fully functional and operate correctly as intended on systems using the US Government Configuration Baseline (USGCB), DISA Security Technical Implementation Guides (STIGs), Center for Information Security (CIS) Security Benchmarks or any other HHS-identified configuration baseline. The standard installation, operation, maintenance, updates, and/or patching of software shall not alter the configuration settings from the approved HHS Vision Platform configuration baseline.

2) The CSP contractor shall use Security Content Automation Protocol (SCAP) validated tools with configuration baseline scanner capability to certify their products operate correctly with HHS and NIST defined configurations and do not alter these settings.

D. Incident Reporting

The Contractor (and/or any subcontractor) shall respond to all alerts/Indicators of Compromise (IOCs) provided by HHS Computer Security Incident Response Center (CSIRC) IRT teams **within 24 hours,** whether the response is positive or negative.

FISMA defines an incident as "an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. The HHS *Policy for IT Security and Privacy Incident Reporting and Response* further defines incidents as events involving cybersecurity and privacy threats, such as viruses, malicious user activity, loss of, unauthorized disclosure or destruction of data, and so on.

A privacy breach is a type of incident and is defined by Federal Information Security Modernization Act (FISMA) as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose. The HHS *Policy for IT Security and Privacy*

Incident Reporting and Response further defines a breach as "a suspected or confirmed incident involving PII".

In the event of a suspected or confirmed incident or breach, the Contractor (and/or any subcontractor) shall:

1) Vision all sensitive information, including any PII created, stored, or transmitted in the performance of this contract so as to avoid a secondary sensitive information incident with FIPS 140-2 validated encryption.

2) NOT notify affected individuals unless so instructed by the Contracting Officer or designated representative. If so instructed by the Contracting Officer or representative, the Contractor shall send HHS Vision Platform ISSO and Vision Data Sharing Platform COR approved notifications to affected individuals.

3) Report all suspected and confirmed information security and privacy incidents and breaches to the HHS Incident Response Team (IRT), COR, CO, Vision Data Sharing Platform SOP (or his or her designee), and other stakeholders, including incidents involving PII, in any medium or form, including paper, oral, or electronic, as soon as possible and without unreasonable delay, no later than **one (1) hour**, and consistent with the applicable HHS policy and procedures, NIST standards and guidelines, as well as US-CERT notification guidelines. The types of information required in an incident report must include at a minimum: company and point of contact information, contract information, impact classifications/threat vector, and the type of information compromised. In addition, the Contractor shall:

   a. cooperate and exchange any information, as determined by the Agency, necessary to effectively manage or mitigate a suspected or confirmed breach;
   b. not include any sensitive information in the subject or body of any reporting e-mail; and
   c. encrypt sensitive information in attachments to email, media, etc.

4) Comply with OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* HHS incident response policies when handling PII breaches.

5) Provide full access and cooperate on all activities as determined by the Government to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents. This may involve disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls. This may also involve physical access to contractor facilities during a breach/incident investigation.

6) The Contractor (and/or any subcontractor) shall provide an Incident and Breach Response Plan (IRP) in accordance with HHS, OMB, and US-CERT requirements and obtain approval from the

Vision Data Sharing Platform. In addition, the Contractor must follow the incident response and US-CERT reporting guidance contained in the HHS Incident Communications.

7) The Contractor (and/or any subcontractor) must implement a program of inspection to safeguard against threats and hazards to the security, confidentiality, integrity, and availability of federal data, afford HHS access to its facilities, installations, technical capabilities, operations, documentation, records, and databases within ***72 hours*** of notification. The program of inspection shall include, but is not limited to:

a. Conduct authenticated and unauthenticated operating system/network/database/Web application vulnerability scans. Automated scans can be performed by HHS personnel, or agents acting on behalf of HHS, using agency-operated equipment and/or specified tools. The Contractor may choose to run its own automated scans or audits, provided the scanning tools and configuration settings are compliant with NIST Security Content Automation Protocol (SCAP) standards and have been approved by the agency. The agency may request the Contractor's scanning results and, at the agency discretion, accept those in lieu of agency performed vulnerability scans.

b. In the event an incident involving sensitive information occurs, cooperate on all required activities determined by the agency to ensure an effective incident or breach response and provide all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents. In addition, the Contractor must follow the agency reporting procedures and document the steps it takes to contain and eradicate the incident, recover from the incident, and provide a post-incident report that includes at a minimum the following:
   - Company and point of contact name;
   - Contract information;
   - Impact classifications/threat vector;
   - Type of information compromised;
   - A summary of lessons learned; and
   - Explanation of the mitigation steps of exploited vulnerabilities to prevent similar incidents in the future.

E. Media Transport

1) The Contractor and its employees shall be accountable and document all activities associated with the transport of government information, devices, and media transported outside controlled areas and/or facilities. These include information stored on digital and non-digital media (e.g., CD-ROM, tapes, etc.), mobile/portable devices (e.g., USB flash drives, external hard drives, and SD cards).
2) All information, devices and media must be encrypted with HHS-approved encryption mechanisms to Vision the confidentiality, integrity, and availability of all government information transported outside of controlled facilities.

F. Boundary Protection: Trusted Internet Connections (TIC)

1) The contractor shall ensure that government information, other than unrestricted information, being transmitted from federal government entities to external entities using cloud services is inspected by Trusted Internet Connection (TIC) processes.

2) The contractor shall route all external connections through a TIC.
3) **Non-Repudiation.** The contractor shall provide a system that implements FIPS 140-2 validated encryption that provides for origin authentication, data integrity, and signer non-repudiation.

a. Information Technology Application Design, Development, or Support

1) The Contractor (and/or any subcontractor) shall ensure IT applications designed and developed for end users (including mobile applications and software licenses) run in the standard user context without requiring elevated administrative privileges.

2) The Contractor (and/or any subcontractor) shall follow secure coding best practice requirements, as directed by United States Computer Emergency Readiness Team (US-CERT) specified standards and the Open Web Application Security Project (OWASP), that will limit system software vulnerability exploits.

3) The Contractor (and/or any subcontractor) shall ensure that computer software developed on behalf of HHS or tailored from an open-source product, is fully functional and operates correctly on systems configured in accordance with government policy and federal configuration standards. The contractor shall test applicable products and versions with all relevant and current updates and patches updated prior to installing in the HHS environment. No sensitive data shall be used during software testing.

4) The Contractor (and/or any subcontractor) shall Vision information that is deemed sensitive from unauthorized disclosure to persons, organizations or subcontractors who do not have a need to know the information. Information which, either alone or when compared with other reasonably-available information, is deemed sensitive or proprietary by HHS shall be protected as instructed in accordance with the magnitude of the loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. This language also applies to all subcontractors that are performing under this contract.

4.6 INCIDENT REPORTING

The Contractor (and/or any subcontractor) shall maintain an Incident and Breach Response Plan (IRP) in accordance with HHS, OMB, and US-CERT requirements.

4.7 PROHIBITION AGAINST PERSONAL SERVICES

The Contractor shall not perform personal services under this contract. Contractor personnel are employees of the Contractor or its subcontractors and are under the administrative control and supervision of the Contractor. A Contractor supervisor must give all individual Contractor employee assignments and daily work direction. The Government will not supervise or direct Contractor employees in the performance of their assignments. If at any time the Contractor believes that any Government action or communication has been given that would create a personal service relationship

between the Government and any Contractor employee, the contractor shall promptly notify the Contracting Officer of this communication or action. The Contractor shall not perform any inherently-governmental functions under this contract. No Contractor employee shall represent or give the appearance that he/she is a Government employee, agent or representative. No Contractor employee shall state orally or in writing at any time that he or she is acting on behalf of the Government. The Contractor is responsible for ensuring that all employees assigned to this contract understand and are committed to following these requirements.

4.8 POST AWARD ORGANIZATIONAL CONFLICT OF INTEREST

a. General: The Contractor shall have programs in place to identify, report, and mitigate actual and potential conflicts of interest for itself, its employees, subcontractors and consultants. The existence of such programs and the disclosure of known actual or potential conflicts are material performance requirements of this contract.

b. Disclosure: The Contractor shall report all actual and potential conflicts of interest pertaining to this contract to the Contracting Officer, including those that would be caused by a contemplated modification to this contact or another contract. Such reports shall be in writing (including by email). Upon request, the Contractor shall respond to a Contracting Officer's request for an OCI mitigation plan.

c. Resolution: In the event the Contracting Officer determines that a conflict of interest exists, based on disclosure from the Contractor or from other sources, the Contracting Officer shall take action which may include, but is not limited to, requesting a mitigation plan from the Contractor, terminating part or all of the contract, modifying the contract or obtaining a waiver in accordance with applicable law, including FAR 9.503 as applicable.

4.9 INFORMATION SECURITY AND/OR PHYSICAL ACCESS SECURITY REQUIREMENTS

A. Baseline Security Requirements

1) **Applicability.** The requirements herein apply whether the entire contract or order (hereafter "contract"), or portion thereof, includes either or both of the following:
   a. Access (Physical or Logical) to Government Information: A Contractor (and/or any subcontractor) employee will have or will be given the ability to have, routine physical (entry) or logical (electronic) access to government information.
   b. Operate a Federal System Containing Information: A Contractor (and/or any subcontractor) will operate a federal system and information technology containing data that supports the HHS mission. In addition to the Federal Acquisition Regulation (FAR) Subpart 2.1 definition of "information technology" (IT), the term as used in this section includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources.
2) **Safeguarding Information and Information Systems**. In accordance with the Federal Information Processing Standards Publication (FIPS)199, *Standards for Security Categorization of Federal Information and Information Systems*, the Contractor (and/or any subcontractor) shall:

a. Vision government information and information systems in order to ensure:
   - **Confidentiality**, which means preserving authorized restrictions on access and disclosure, based on the security terms found in this contract, including means for protecting personal privacy and proprietary information;
   - **Integrity**, which means guarding against improper information modification or destruction, and ensuring information non-repudiation and authenticity; and
   - **Availability**, which means ensuring timely and reliable access to and use of information.

b. Provide security for any Contractor systems, and information contained therein, connected to an HHS network or operated by the Contractor on behalf of HHS regardless of location. In addition, if new or unanticipated threats or hazards are discovered by either the agency or contractor, or if existing safeguards have ceased to function, the discoverer shall immediately, **within one (1) hour or less**, bring the situation to the attention of the other party.

c. Adopt and implement the policies, procedures, controls, and standards required by the HHS Information Security Program to ensure the confidentiality, integrity, and availability of government information and government information systems for which the Contractor is responsible under this contract or to which the Contractor may otherwise have access under this contract. Obtain the HHS Information Security Program security requirements, outlined in the HHS Information Security and Privacy Policy (IS2P), by contacting the CO/COR or emailing fisma@hhs.gov.

d. Comply with the Privacy Act requirements and tailor FAR clauses as needed..

3) **Information Security Categorization**. In accordance with FIPS 199 and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60, *Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*, Appendix C, and based on information provided by the ISSO, CISO, or other security representative, the risk level for each Security Objective and the Overall Risk Level, which is the highest watermark of the three factors (Confidentiality, Integrity, and Availability) of the information or information system are the following:

Confidentiality:	[ ] Low [X] Moderate [ ] High
Integrity:	[ ] Low [X] Moderate [ ] High
Availability:	[ ] Low [X] Moderate [ ] High
Overall Risk Level:	[ ] Low [X] Moderate [ ] High

Based on information provided by the ISSO, Privacy Office, system/data owner, or other security or privacy representative, it has been determined that this solicitation/contract involves:

[X] No PII [ ] Yes PII

Personally Identifiable Information (PII). Per the Office of Management and Budget (OMB) Circular A-130, "PII is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." Examples of PII include, but are not limited to the following: social security number, date and place of birth, mother's maiden name, biometric records, etc.

PII Confidentiality Impact Level has been determined to be: [ ] Low [X] Moderate [ ] High

4) **Controlled Unclassified Information (CUI).** CUI is defined as "information that laws, regulations, or Government-wide policies require to have safeguarding or dissemination controls, excluding classified information." The Contractor (and/or any subcontractor) must comply with *Executive Order 13556, Controlled Unclassified Information, (implemented at 3 CFR,* part 2002*)* when handling CUI. 32 C.F.R. 2002.4(aa) As implemented the term "h*andling"* refers to "…any use of CUI, including but not limited to marking, safeguarding, transporting, disseminating, re-using, and disposing of the information." 81 Fed. Reg. 63323. All sensitive information that has been identified as CUI by a regulation or statute, handled by this solicitation/contract, shall be:
    a. marked appropriately;
    b. disclosed to authorized personnel on a Need-To-Know basis;
    c. protected in accordance with NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* applicable baseline if handled by a Contractor system operated on behalf of the agency, or NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations* if handled by internal Contractor system; and
    d. returned to HHS control, destroyed when no longer needed, or held until otherwise directed. Destruction of information and/or data shall be accomplished in accordance with NIST SP 800-88*, Guidelines for Media Sanitization*.
5) **Protection of Sensitive Information**. For security purposes, information is *or* may be sensitive because it requires security to Vision its confidentiality, integrity, and/or availability. The Contractor (and/or any subcontractor) shall Vision all government information that is or may be sensitive in accordance with OMB Memorandum M-06-16, *Protection of Sensitive Agency Information* by securing it with a FIPS 140-2 validated solution.
6) **Confidentiality and Nondisclosure of Information.** Any information provided to the contractor (and/or any subcontractor) by HHS or collected by the contractor on behalf of HHS shall be used only for the purpose of carrying out the provisions of this contract and shall not be disclosed or made known in any manner to any persons except as may be necessary in the performance of the contract. The Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its employees and subcontractors shall be under the supervision of the Contractor. Each Contractor employee or any of its subcontractors to whom any HHS records may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such employee or subcontractor can be used only for that purpose and to the extent authorized herein.

The confidentiality, integrity, and availability of such information shall be protected in accordance with HHS policies. Unauthorized disclosure of information will be subject to the HHS sanction policies and/or governed by the following laws and regulations:

a. 18 U.S.C. 641 (Criminal Code: Public Money, Property or Records);
b. 18 U.S.C. 1905 (Criminal Code: Disclosure of Confidential Information); and
c. 44 U.S.C. Chapter 35, Subchapter I (Paperwork Reduction Act).

7) **Internet Protocol Version 6 (IPv6).** All procurements using Internet Protocol shall comply with OMB Memorandum M-05-22, *Transition Planning for Internet Protocol Version 6 (IPv6)*.

8) **Government Websites.** All new and existing public-facing government websites must be securely configured with Hypertext Transfer Protocol Secure (HTTPS) using the most recent version of Transport Layer Security (TLS). In addition, HTTPS shall enable HTTP Strict Transport Security (HSTS) to instruct compliant browsers to assume HTTPS at all times to reduce the number of insecure redirects and Vision against attacks that attempt to downgrade connections to plain HTTP. For internal-facing websites, the HTTPS is not required, but it is highly recommended.
9) **Contract Documentation**. The Contractor shall use provided templates, policies, forms and other agency documents to comply with contract deliverables as appropriate.
10) **Standard for Encryption.** The Contractor (and/or any subcontractor) shall:
    a. Comply with the *HHS Standard for Encryption of Computing Devices and Information* to prevent unauthorized access to government information.
    b. Encrypt all sensitive federal data and information (i.e., PII, protected health information [PHI], proprietary information, etc.) in transit (i.e., email, network connections, etc.) and at rest (i.e., servers, storage devices, mobile devices, backup media, etc.) with FIPS 140-2 validated encryption solution.
    c. Secure all devices (i.e.: desktops, laptops, mobile devices, etc.) that store and process government information and ensure devices meet HHS-specific encryption standard requirements. Maintain a complete and current inventory of all laptop computers, desktop computers, and other mobile devices and portable media that store or process sensitive government information (including PII).
    d. Verify that the encryption solutions in use have been validated under the Cryptographic Module Validation Program to confirm compliance with FIPS 140-2. The Contractor shall provide a written copy of the validation documentation to the COR.
    e. Use the Key Management system on the HHS personal identification verification (PIV) card or establish and use a key recovery mechanism to ensure the ability for authorized personnel to encrypt/decrypt information and recover encryption keys. Encryption keys shall be provided to the COR upon request and at the conclusion of the contract.
11) **Contractor Non-Disclosure Agreement (NDA)**. Each Contractor (and/or any subcontractor) employee having access to non-public government information under this contract shall complete the Vision Data Sharing Platform non-disclosure agreement, as applicable. A copy of each signed and witnessed NDA shall be submitted to the Contracting Officer (CO) and/or CO Representative (COR) prior to performing any work under this acquisition.
12) **Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA)** – The Contractor shall assist the Vision Data Sharing Platform Senior Official for Privacy (SOP) or designee with conducting a PTA for the information system and/or information handled under this contract to determine whether or not a full PIA needs to be completed.
    a. If the results of the PTA show that a full PIA is needed, the Contractor shall assist the Vision Data Sharing Platform SOP or designee with completing a PIA for the system or information as agreed or after completion of the PTA and in accordance with HHS policy and OMB M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*.
    b. The Contractor shall assist the Vision Data Sharing Platform SOP or designee in reviewing the PIA at least every ***three years*** throughout the system development lifecycle (SDLC)/information lifecycle, or when determined by the agency that a review is required based on a major change to the system, or when new types of PII are collected that

introduces new or increased privacy risks, whichever comes first.

Training

1) **Mandatory Training for All Contractor Staff.** All Contractor (and/or any subcontractor) employees assigned to work on this contract shall complete the applicable HHS Contractor Information Security Awareness, Privacy, and Records Management training (provided upon contract award) before performing any work under this contract. Thereafter, the employees shall complete HHS Information Security Awareness, Privacy, and Records Management training at least ***annually***, during the life of this contract. All provided training shall be compliant with HHS training policies.
2) **Role-based Training.** All Contractor (and/or any subcontractor) employees with significant security responsibilities (as determined by the program manager) must complete role-based training ***annually*** commensurate with their role and responsibilities in accordance with HHS policy and the *HHS Role-Based Training (RBT) of Personnel with Significant Security Responsibilities Memorandum*.
3) **Training Records.** The Contractor (and/or any subcontractor) shall maintain training records for all its employees working under this contract in accordance with HHS policy. A copy of the training records shall be provided to the CO and/or COR within ***30 days*** after contract award and ***annually*** thereafter or upon request.

Rules of Behavior

1) The Contractor (and/or any subcontractor) shall ensure that all employees performing on the contract comply with the *HHS Information Technology General Rules of Behavior*.
2) All Contractor employees performing on the contract must read and adhere to the Rules of Behavior before accessing Department data or other information, systems, and/or networks that store/process government information, initially at the beginning of the contract and at least ***annually*** thereafter, which may be done as part of annual HHS Information Security Awareness Training. If the training is provided by the contractor, the signed ROB must be provided as a separate deliverable to the CO and/or COR per defined timelines above.

Incident Response

The Contractor (and/or any subcontractor) shall respond to all alerts/Indicators of Compromise (IOCs) provided by HHS Computer Security Incident Response Center (CSIRC) IRT teams **within 24 hours,** whether the response is positive or negative.

FISMA defines an incident as "an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.. The HHS *Policy for IT Security and Privacy Incident Reporting and Response* further defines incidents as events involving cybersecurity and privacy threats, such as viruses, malicious user activity, loss of, unauthorized disclosure or destruction of data, and so on.

A privacy breach is a type of incident and is defined by Federal Information Security Modernization Act (FISMA) as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose. The HHS *Policy for IT Security and Privacy*

Incident Reporting and Response further defines a breach as "a suspected or confirmed incident involving PII".

In the event of a suspected or confirmed incident or breach, the Contractor (and/or any subcontractor) shall:

1) Vision all sensitive information, including any PII created, stored, or transmitted in the performance of this contract so as to avoid a secondary sensitive information incident with FIPS 140-2 validated encryption.
2) NOT notify affected individuals unless so instructed by the Contracting Officer or designated representative. If so instructed by the Contracting Officer or representative, the Contractor shall send HHS Vision Platform ISSO and Vision Data Sharing Platform COR approved notifications to affected individuals.
3) Report all suspected and confirmed information security and privacy incidents and breaches to the HHS Incident Response Team (IRT), COR, CO, Vision Data Sharing Platform SOP (or his or her designee), and other stakeholders, including incidents involving PII, in any medium or form, including paper, oral, or electronic, as soon as possible and without unreasonable delay, no later than **one (1) hour**, and consistent with the applicable HHS policy and procedures, NIST standards and guidelines, as well as US-CERT notification guidelines. The types of information required in an incident report must include at a minimum: company and point of contact information, contract information, impact classifications/threat vector, and the type of information compromised. In addition, the Contractor shall:
    d. cooperate and exchange any information, as determined by the Agency, necessary to effectively manage or mitigate a suspected or confirmed breach;
    e. not include any sensitive information in the subject or body of any reporting e-mail; and
    f. encrypt sensitive information in attachments to email, media, etc.
4) Comply with OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* HHS incident response policies when handling PII breaches.
5) Provide full access and cooperate on all activities as determined by the Government to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents. This may involve disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls. This may also involve physical access to contractor facilities during a breach/incident investigation.

Position Sensitivity Designations

All Contractor (and/or any subcontractor) employees must obtain a background investigation commensurate with their position sensitivity designation that complies with Parts 1400 and 731 of Title 5, Code of Federal Regulations (CFR). The following position sensitivity designation levels apply to this solicitation/contract:

See C.8 for details

Homeland Security Presidential Directive (HSPD)-12

The Contractor (and/or any subcontractor) and its employees shall comply with Homeland Security Presidential Directive (HSPD)-12, *Policy for a Common Identification Standard for Federal Employees*

and Contractors; OMB M-05-24; FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*; HHS HSPD-12 policy; and *Executive Order 13467, Part 1 §1.2.*

Roster. The Contractor (and/or any subcontractor) shall submit a roster by name, position, e-mail address, phone number and responsibility, of all staff working under this acquisition where the Contractor will develop, have the ability to access, or host and/or maintain a government information system(s). The roster shall be submitted to the COR and/or CO within *10 days* of the effective date of this contract. Any revisions to the roster as a result of staffing changes shall be submitted within *5 days* of the change. The COR will notify the Contractor of the appropriate level of investigation required for each staff member.

If the employee is filling a new position, the Contractor shall provide a position description and the Government will determine the appropriate suitability level.

Contract Initiation and Expiration

2) **General Security Requirements.** The Contractor (and/or any subcontractor) shall comply with information security and privacy requirements, Enterprise Performance Life Cycle (EPLC) processes, HHS Enterprise Architecture requirements to ensure information is appropriately protected from initiation to expiration of the contract. All information systems development or enhancement tasks supported by the contractor shall follow the HHS EPLC framework and methodology and in accordance with the HHS Contract Closeout Guide (2012).

HHS EA requirements may be located here: https://www.hhs.gov/ocio/ea/documents/proplans.html

3) **System Documentation.** Contractors (and/or any subcontractors) must follow and adhere to NIST SP 800-64, *Security Considerations in the System Development Life Cycle*, at a minimum, for system development and provide system documentation at designated intervals (specifically, at the expiration of the contract) within the EPLC that require artifact review and approval.
4) **Sanitization of Government Files and Information.** As part of contract closeout and at expiration of the contract, the Contractor (and/or any subcontractor) shall provide all required documentation to the CO and/or COR to certify that, at the government's direction, all electronic and paper records are appropriately disposed of and all devices and media are sanitized in accordance with NIST SP 800-88, *Guidelines for Media Sanitization*.
5) **Notification.** The Contractor (and/or any subcontractor) shall notify the CO and/or COR and system ISSO within *5 days* before an employee stops working under this contract.
6) **Contractor Responsibilities Upon Physical Completion of the Contract**. The contractor (and/or any subcontractors) shall return all government information and IT resources (i.e., government information in non-government-owned systems, media, and backup systems) acquired during the term of this contract to the CO and/or COR. Additionally, the Contractor shall provide a certification that all government information has been properly sanitized and purged from Contractor-owned systems, including backup systems and media used during contract performance, in accordance with HHS and/or *Vision Data Sharing Platform* policies.
7) The Contractor (and/or any subcontractor) shall perform and document the actions identified in the ***HHS*** Contractor Employee Separation Checklist when an employee terminates work under this contract within 2 working days of the employee's exit from the contract. All documentation shall be made available to the CO and/or COR upon request.

RECORDS MANAGEMENT AND RETENTION

The Contractor (and/or any subcontractor) shall maintain all information in accordance with Executive Order 13556 -- Controlled Unclassified Information, National Archives and Records Administration (NARA) records retention policies and schedules and HHS / OS policies and shall not dispose of any records unless authorized by HHS / OS.

In the event that a Contractor (and/or any subcontractor) accidentally disposes of or destroys a record without proper authorization, it shall be documented and reported as an incident in accordance with HHS / OS policies.

4.10 REQUIREMENTS FOR PRIVACY ACT RECORDS

It has been determined that this contract is subject to the Privacy Act of 1974, should the contractor encounter the design, development, or operation of a system of records on individuals.

The System of Records Notice (SORN) that is applicable to this contract is: *EHRP/Vision Data Sharing Platform*

The design, development, or operation work the Contractor is to perform is Vision Data Sharing Platform.

The disposition to be made of the Privacy Act records upon completion of contract performance is: *as defined by HHS Privacy and Vision Data Sharing Platform policy and will be modified into this contract.*

4.11 REQUIREMENTS FOR GOVERNMENT INFORMATION PROCESSED ON GOCO OR COCO SYSTEMS

Security Requirements for GOCO and COCO Resources

1) **Federal Policies.** The Contractor (and/or any subcontractor) shall comply with applicable federal laws that include, but are not limited to, the *HHS Information Security and Privacy Policy (IS2P)*, *Federal Information Security Modernization Act (FISMA) of 2014, (44 U.S.C. 101)*; National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and* Organizations; Office of Management and Budget (OMB) Circular A-130*, Managing Information as a Strategic Resource*; and other applicable federal laws, regulations, NIST guidance, and Departmental policies.
2) **Security Assessment and Authorization (SA&A)**. A valid authority to operate (ATO) certifies that the Contractor's information system meets the contract's requirements to Vision the agency data. If the system under this contract does not have a valid ATO, the Contractor (and/or any subcontractor) shall work with the agency and supply the deliverables required to complete the ATO within the specified timeline(s) as agreed to by the COR. The Contractor shall conduct the SA&A requirements in accordance with *HHS IS2P,* NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (latest revision).

HHS acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the system security and privacy controls are implemented and operating effectively.

a. SA&A Package Deliverables - The Contractor (and/or any subcontractor) shall provide an SA&A package within *outlined in the project management plan* to the CO and/or COR. The following SA&A deliverables are required to complete the SA&A package.
   - **System Security Plan (SSP)** – The SSP shall comply with the NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, the Federal Information Processing Standard (FIPS) 200, *Recommended Security Controls for Federal Information Systems*, and NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* applicable baseline requirements, and other applicable NIST guidance as well as HHS policies and other guidance. The SSP shall be consistent with and detail the approach to IT security contained in the Contractor's bid or quote that resulted in the award of this contract. The SSP shall provide an overview of the system environment and security requirements to Vision the information system as well as describe all applicable security controls in place or planned for meeting those requirements. It should provide a structured process for planning adequate, cost-effective security protection for a system. The Contractor shall update the SSP at least ***annually*** thereafter.
   - **Security Assessment Plan/Report (SAP/SAR)** –The security assessment shall be conducted by HHS assessor and be consistent with NIST SP 800-53A, NIST SP 800-30, and HHS policies. The assessor will document the Vision Data Sharing Platform assessment results in the SAR.

Thereafter, the Contractor, in coordination with ***Vision Data Sharing Platform*** shall *assist* in the assessment of the security controls and update the SAR at least ***annually***.

   - **Independent Assessment –** If appropriate the Contractor (and/or subcontractor) shall have an independent third-party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the Security Authorization package, and report on technical, operational, and management level deficiencies as outlined in NIST SP 800-53. The Contractor shall address all *"high"* deficiencies before submitting the package to the Government for acceptance. All remaining deficiencies must be documented in a system Plan of Actions and Milestones (POA&M).
   - **POA&M** – The POA&M shall be documented consistent with the HHS Standard for Plan of Action and Milestones and policies. All high-risk weaknesses must be mitigated within *HHS timeframes as agreed and documented in the project management plan* and all medium weaknesses must be mitigated within *the timeframe as agreed and documented in the project management plan* from the date the weaknesses are formally identified and documented. *Vision Data Sharing Platform* will determine the risk rating of vulnerabilities.

Identified risks stemming from deficiencies related to the security control baseline implementation, assessment, continuous monitoring, vulnerability scanning, and other security reviews and sources, as documented in the SAR, shall be documented and tracked by the Contractor for mitigation in the POA&M document. Depending on the severity of the risks, ***Vision Data Sharing Platform*** may require designated POAM weaknesses to be remediated before an ATO is issued. Thereafter, the POA&M shall be updated at least ***quarterly***.

   - **Contingency Plan and Contingency Plan Test** – The Contingency Plan must be developed in accordance with NIST SP 800-34, *Contingency Planning Guide for Federal Information*

Systems, and be consistent with HHS policies. Upon acceptance by the System Owner, the Contractor, in coordination with the System Owner, shall test the Contingency Plan and prepare a Contingency Plan Test Report that includes the test results, lessons learned and any action items that need to be addressed. Thereafter, the Contractor shall update and test the Contingency Plan at least ***annually***.

- **E-Authentication Questionnaire** – The contractor (and/or any subcontractor) shall collaborate with government personnel to ensure that an E-Authentication Threshold Analysis (E-auth TA) is completed to determine if a full E-Authentication Risk Assessment (E-auth RA) is necessary. System documentation developed for a system using E-auth TA/E-auth RA methods shall follow OMB 04-04 and NIST SP 800-63, Rev. 2, *Electronic Authentication Guidelines*.

Based on the level of assurance determined by the E-Auth, the Contractor (and/or subcontractor) must ensure appropriate authentication to the system, including remote authentication, is in-place in accordance with the assurance level determined by the E-Auth (when required) in accordance with HHS policies.

b. Information Security Continuous Monitoring. Upon the government issuance of an Authority to Operate (ATO), the Contractor (and/or subcontractor)-owned/operated systems that input, store, process, output, and/or transmit government information, shall meet or exceed the information security continuous monitoring (ISCM) requirements in accordance with FISMA and NIST SP 800-137*, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, and HHS IS2P. The following are the minimum requirements for ISCM:

- **Annual Assessment/Pen Test -** Assess the system security and privacy controls (or ensure an assessment of the controls is conducted) at least annually to determine the implemented security and privacy controls are operating as intended and producing the desired results (this may involve penetration testing conducted by the agency or independent third-party.) In addition, review all relevant SA&A documentation (SSP, POA&M, Contingency Plan, etc.) and provide updates as required.
- **Asset Management -** Using any available Security Content Automation Protocol (SCAP)-compliant automated tools for active/passive scans, provide an inventory of all information technology (IT) assets for hardware and software, (computers, servers, routers, databases, operating systems, etc.) that are processing HHS-owned information/data. It is anticipated that this inventory information will be required to be produced at least *quarterly by the CSP*. IT asset inventory information shall include IP address, machine name, operating system level, security patch level, and SCAP-compliant format information. The contractor shall maintain a capability to provide an inventory of 100% of its IT assets using SCAP-compliant automated tools.
- **Configuration Management** - Use available SCAP-compliant automated tools, per NIST IR 7511, for authenticated scans to provide visibility into the security configuration compliance status of all IT assets, (computers, servers, routers, databases, operating systems, application, etc.) that store and process government information. Compliance will be measured using IT assets and standard HHS and government configuration baselines at least *quarterly by the CSP.* The CSP contractor shall maintain a capability to provide security configuration compliance information for 100% of its IT assets using SCAP-compliant automated tools.
- **Vulnerability Management –** The CSP shall use SCAP-compliant automated tools for authenticated scans to scan information system(s) and detect any security vulnerabilities in all assets (computers, servers, routers, Web applications, databases, operating systems, etc.) that

store and process government information. Contractors shall actively manage system vulnerabilities using automated tools and technologies where practicable and in accordance with HHS policy. Automated tools shall be compliant with NIST-specified SCAP standards for vulnerability identification and management. The contractor shall maintain a capability to provide security vulnerability scanning information for 100% of IT assets using SCAP-compliant automated tools and report to the agency at least *quarterly*.

- **Patching and Vulnerability Remediation** - Install vendor released security patches and remediate critical and high vulnerabilities in systems processing government information in an expedited manner, within vendor and agency specified timeframes *by the CSP in coordination with Vision Data Sharing Platform PMO and ISSO.*
- **Secure Coding** - Follow secure coding best practice requirements, as directed by United States Computer Emergency Readiness Team (US-CERT) specified standards and the Open Web Application Security Project (OWASP), that will limit system software vulnerability exploits.
- **Boundary Protection** - The contractor shall ensure that government information, other than unrestricted information, being transmitted from federal government entities to external entities is routed through a Trusted Internet Connection (TIC).

3) **Government Access for Security Assessment**. In addition to the Inspection Clause in the contract, the Contractor (and/or any subcontractor) shall afford the Government access to the Contractor's facilities, installations, operations, documentation, information systems, and personnel used in performance of this contract to the extent required to carry out a program of security assessment (to include vulnerability testing), investigation, and audit to safeguard against threats and hazards to the confidentiality, integrity, and availability of federal data or to the protection of information systems operated on behalf of HHS, including but are not limited to:

a. At any tier handling or accessing information, consent to and allow the Government, or an independent third party working at the Government's direction, without notice at any time during a weekday during regular business hours contractor local time, to access contractor and subcontractor installations, facilities, infrastructure, data centers, equipment (including but not limited to all servers, computing devices, and portable media), operations, documentation (whether in electronic, paper, or other forms), databases, and personnel which are used in performance of the contract.

The Government includes but is not limited to the U.S. Department of Justice, U.S. Government Accountability Office, and the HHS Office of the Inspector General (OIG). The purpose of the access is to facilitate performance inspections and reviews, security and compliance audits, and law enforcement investigations. For security audits, the audit may include but not be limited to such items as buffer overflows, open ports, unnecessary services, lack of user input filtering, cross site scripting vulnerabilities, SQL injection vulnerabilities, and any other known vulnerabilities.

b. At any tier handling or accessing protected information, fully cooperate with all audits, inspections, investigations, forensic analysis, or other reviews or requirements needed to carry out requirements presented in applicable law or policy. Beyond providing access, full cooperation also includes, but is not limited to, disclosure to investigators of information sufficient to identify the nature and extent of any criminal or fraudulent activity and the individuals responsible for that activity. It includes timely and complete production of requested data, metadata, information, and records relevant to any inspection, audit, investigation, or review, and making employees of the contractor available for interview by

inspectors, auditors, and investigators upon request. Full cooperation also includes allowing the Government to make reproductions or copies of information and equipment, including, if necessary, collecting a machine or system image capture.

c. Segregate Government protected information and metadata on the handling of Government protected information from other information. Commingling of information is prohibited. Inspectors, auditors, and investigators will not be precluded from having access to the sought information if sought information is commingled with other information.
d. Cooperate with inspections, audits, investigations, and reviews.

4) **End of Life Compliance.** The Contractor (and/or any subcontractor) must use Commercial off the Shelf (COTS) software or other software that is supported by the manufacturer. In addition, the COTS/other software need to be within one major version of the current version; deviation from this requirement will only be allowed via the HHS waiver process (approved by HHS CISO). The contractor shall retire and/or upgrade all software/systems that have reached end-of-life in accordance with HHS *End-of-Life Operating Systems, Software, and Applications Policy*.
5) **Desktops, Laptops, and Other Computing Devices Required for Use by the Contractor**. The Contractor (and/or any subcontractor) shall ensure that all IT equipment (e.g., laptops, desktops, servers, routers, mobile devices, peripheral devices, etc.) used to process information on behalf of HHS are deployed and operated in accordance with approved security configurations and meet the following minimum requirements:
    a. Encrypt equipment and sensitive information stored and/or processed by such equipment in accordance with HHS and FIPS 140-2 encryption standards.
    b. Configure laptops and desktops in accordance with the latest applicable United States Government Configuration Baseline (USGCB) and HHS *Minimum Security Configuration Standards*;
    c. Maintain the latest operating system patch release and anti-virus software definitions;
    d. Validate the configuration settings after hardware and software installation, operation, maintenance, update, and patching and ensure changes in hardware and software do not alter the approved configuration settings; and
    e. Automate configuration settings and configuration management in accordance with HHS security policies, including but not limited to:
        - Configuring its systems to allow for periodic HHS vulnerability and security configuration assessment scanning; and
        - Using Security Content Automation Protocol (SCAP)-validated tools with USGCB Scanner capabilities to scan its systems at least on a ***monthly*** basis and report the results of these scans to the CO and/or COR, Project Officer, and any other applicable designated POC.

4.12 INFORMATION TECHNOLOGY APPLICATION DESIGN, DEVELOPEMNT, OR SUPPORT

1) The Contractor (and/or any subcontractor) shall ensure IT applications designed and developed for end users (including mobile applications and software licenses) run in the standard user context without requiring elevated administrative privileges.

2) The Contractor (and/or any subcontractor) shall follow secure coding best practice requirements, as directed by United States Computer Emergency Readiness Team (US-CERT) specified standards and the Open Web Application Security Project (OWASP), that will limit system software vulnerability exploits.

3) The Contractor (and/or any subcontractor) shall ensure that computer software developed on behalf of HHS or tailored from an open-source product, is fully functional and operates correctly on systems configured in accordance with government policy and federal configuration standards. The contractor shall test applicable products and versions with all relevant and current updates and patches updated prior to installing in the HHS environment. No sensitive data shall be used during software testing.

4) The Contractor (and/or any subcontractor) shall protect information that is deemed sensitive from unauthorized disclosure to persons, organizations or subcontractors who do not have a need to know the information. Information which, either alone or when compared with other reasonably-available information, is deemed sensitive or proprietary by HHS shall be protected as instructed in accordance with the magnitude of the loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. This language also applies to all subcontractors that are performing under this contract.

4.13 GOVERNMENT SUPPORT

HHS-OCIO will evaluate whether development work can be performed on Contractor furnished equipment. If the decision is no, then HHS-OCIO will provide Government Furnished Equipment for all Contractors.

4.14 PRIORITIES AND ALLOCATIONS

HHS reserves the right to exercise priorities and allocations authority with respect to this contract, to include rating this order in accordance with 45 CFR Part 101, Subpart A—Health Resources Priorities and Allocations System.

4.15HHSAR 352.239-73(b) Electronic and Information Technology Accessibility (January 2010)

(a) Pursuant to Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998, all electronic and information technology (EIT) products and services developed, acquired, maintained, or used under this contract/order must comply with the "Electronic and Information Technology Accessibility Provisions" set forth by the Architectural and Transportation Barriers Compliance Board (also referred to as the "Access Board") in 36 CFR Part 1194. Information about Section 508 is available at http://www.section508.gov/. The complete text of Section 508 Final Provisions can be accessed at http://www.access-board.gov/sec508/standards.htm.

(b) The Section 508 accessibility standards applicable to this contract/order are identified in the Statement of Work/Specification/Performance Work Statement. The Contractor must provide a written Section 508 conformance certification due at the end of each contract/order exceeding $150,000 when the contract/order duration is one year or less. If it is determined by the Government that EIT products and services provided by the Contractor do not conform to the described accessibility standards in the Product Assessment Template, remediation of the products or services to the level of conformance specified in the Contractor's Product Assessment Template will be the responsibility of the Contractor at its own expense.
(c) In the event of a modification(s) to this contract/order, which adds new EIT products or services or revises the type of, or specifications for, products or services the Contractor is to provide, including EIT deliverables such as electronic documents and reports, the Contracting Officer may require that the contractor submit a completed HHS Section 508 Product Assessment Template to assist the Government in determining that the EIT products or services support Section 508 accessibility standards. Instructions for documenting accessibility via the HHS Section 508 Product Assessment Template may be found under Section 508 policy on the HHS Office on Disability website (http://www.hhs.gov/od/).

Prior to the Contracting Officer exercising an option for a subsequent performance period/additional quantity or adding funding for a subsequent performance period under this contract, as applicable, the Contractor must provide a Section 508 Annual Report to the Contracting Officer and Project Officer. Unless otherwise directed by the Contracting Officer in writing, the Contractor shall provide the cited report in accordance with the following schedule. Instructions for completing the report are available in the Section 508 policy on the HHS Office on Disability website under the heading Vendor Information and Documents. The Contractor's failure to submit a timely and properly completed report may jeopardize the Contracting Officer's exercising an option or adding funding, as applicable.
Schedule for Contractor Submission of Section 508 Annual Report
(to be completed by the Contracting Officer at time of contract/order award)

4.16HHS SECTION 508 ACCESSIBILITY STANDARDS NOTICE

This contract is subject to Section 508 of the Rehabilitation Act (the Act) of 1973 (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998, and the Architectural and Transportation Barriers Compliance Board (Access Board) Electronic and Information Accessibility Provisions (36 CFR Part 1194). Section 508 of the Act requires that, unless an exception applies, all communications products and services that require a contractor or consultant to produce content in any format that is specifically intended for publication on, or delivery via, a federally owned or federally funded website permit the following:
(1) Federal employees with disabilities to have access to and use information and data that is comparable to the access and use of information and data by federal employees who are not individuals with disabilities.
(2) Members of the public with disabilities seeking information or services from a federal agency to have access to and use of information and data that is comparable to the access and use of information and data by members of the public who are not individuals with disabilities.
(Note: Information about Section 508 of the Act is available at http://www.section508.gov/. The complete text of Section 508 can be accessed at http://www.access-board.gov/sec508/provisions.htm.)

Accordingly, regardless of format, all web content or communications materials specifically produced for publication on, or delivery via, HHS websites, including text, audio, or video, under this contract shall conform to applicable Section 508 accessibility standards. Remediation of any materials that do not comply with the applicable accessibility standards of 36 CFR Part 1194 as set forth herein shall be the responsibility of the Contractor.
The following Section 508 accessibility standards apply to the content or communications material identified in this SOW or PWS:

General (Subpart A)

The standards define the types of technology covered and set forth provisions that establish a minimum level of accessibility. The application section (1194.2) outlines the scope and coverage of the standards. The standards cover the full range of electronic and information technologies in the Federal sector, including those used for communication, duplication, computing, storage, presentation, control, transport and production. This includes computers, software, networks, peripherals and other types of electronic office equipment. The standards define *electronic and information technology*, in part, as "any equipment or interconnected system or subsystem of equipment, that is used in the creation, conversion, or duplication of data or information." Subpart A also explains what is exempt (1194.3), defines terms (1194.4), and generally recognizes alternatives to what is required that provide equal or greater access (1194.5). Consistent with the law, the standards exempt systems used for military command, weaponry, intelligence, and cryptologic activities (but not routine business and administrative systems used for other defense-related purposes or by defense agencies or personnel). The standards also exempt "back office" equipment used only by service personnel for maintenance, repair, or similar purposes. The standards cover technology procured by Federal agencies under contract with a private entity, but apply only to those products directly relevant to the contract and its deliverables. An exception clarifies that the standards do not apply to technology that is incidental to a Federal contract. Thus, those products that are not specified as part of a contract with a Federal agency would not have to comply with the standards. For example, a firm that produces a report for a Federal agency under a contract would not have to procure accessible computers and word processing software even if they were used exclusively for the contract; however, compliance would be required if such products were to become the property of the Federal agency as contract deliverables or if the Federal agency purchased the products to be used by the contractor as part of the project. If a Federal agency contracts with a firm to develop its web site, the standards would apply to the new web site for the agency but not to the firm's own web site.

Technical Standards (Subpart B)

The standards provide criteria specific to various types of technologies, including:

- software applications and operating systems
- web-based information or applications
- telecommunication products
- video and multimedia products
- self contained, closed products (e.g., information kiosks, calculators, and fax machines)
- desktop and portable computers

This section provides technical specifications and performance-based requirements, which focus on the functional capabilities of covered technologies. This dual approach recognizes the dynamic and continually evolving nature of the technology involved as well as the need for clear and specific standards to facilitate compliance. Certain provisions are designed to ensure compatibility with adaptive equipment people with disabilities commonly use for information and communication access, such as screen readers, Braille displays, and TTYs.

Software Applications and Operating Systems (1194.21)

Most of the specifications for software pertain to usability for people with vision impairments. For example, one provision requires alternative keyboard navigation, which is essential for people with vision impairments who cannot rely on pointing devices, such as a mouse. Other provisions address animated displays, color and contrast settings, flash rate, and electronic forms, among others.

Web-based Intranet and Internet Information and Applications (1194.22)

The criteria for web-based technology and information are based on access guidelines developed by the Web Accessibility Initiative of the World Wide Web Consortium. Many of these provisions ensure access for people with vision impairments who rely on various assistive products to access computer-based information, such as screen readers, which translate what's on a computer screen into automated audible output, and refreshable Braille displays. Certain conventions, such as verbal tags or identification of graphics and format devices, like frames, are necessary so that these devices can "read" them for the user in a sensible way. The standards do not prohibit the use of web site graphics or animation. Instead, the standards aim to ensure that such information is also available in an accessible format. Generally, this means use of text labels or descriptors for graphics and certain format elements. (HTML code already provides an "Alt Text" tag for graphics which can serve as a verbal descriptor for graphics). This section also addresses the usability of multimedia presentations, image maps, style sheets, scripting languages, applets and plug-ins, and electronic forms. The standards apply to Federal web sites but not to private sector web sites (unless a site is provided under contract to a Federal agency, in which case only that web site or portion covered by the contract would have to comply). Accessible sites offer significant advantages that go beyond access. For example, those with "text-only" options provide a faster downloading alternative and can facilitate transmission of web-based data to cell phones and personal digital assistants.

Telecommunications Products (1194.23)

The criteria of this section are designed primarily to ensure access to people who are deaf or hard of hearing. This includes compatibility with hearing aids, cochlear implants, assistive listening devices, and TTYs. TTYs are devices that enable people with hearing or speech impairments to communicate over the telephone; they typically include an acoustic coupler for the telephone handset, a simplified keyboard, and a visible message display. One requirement calls for a standard non-acoustic TTY connection point for telecommunication products that allow voice communication but that do provide TTY functionality. Other specifications address adjustable volume controls for output, product interface with hearing technologies, and the usability of keys and controls by people who may have impaired vision or limited dexterity or motor control.

Video or Multimedia Products (1194.24)

Multimedia products involve more than one media and include, but are not limited to, video programs, narrated slide production, and computer generated presentations. Provisions address caption decoder circuitry (for any system with a screen larger than 13 inches) and secondary audio channels for television tuners, including tuner cards for use in computers. The standards also require captioning and audio description for certain training and informational multimedia productions developed or procured by Federal agencies. The standards also provide that viewers be able to turn captioning or video description features on or off.

Self Contained, Closed Products (1194.25)

This section covers products that generally have imbedded software but are often designed in such a way that a user cannot easily attach or install assistive technology. Examples include information kiosks, information transaction machines, copiers, printers, calculators, fax machines, and similar types of products. The standards require that access features be built into the system so users do not have to attach an assistive device to it. Other specifications address mechanisms for private listening (handset or a standard headphone jack), touchscreens, auditory output and adjustable volume controls, and location of controls in accessible reach ranges.

Desktop and Portable Computers (1194.26)

This section focuses on keyboards and other mechanically operated controls, touch screens, use of biometric form of identification, and ports and connectors.

Functional Performance Criteria (Subpart C)

The performance requirements of this section are intended for overall product evaluation and for technologies or components for which there is no specific requirement under the technical standards in Subpart B. These criteria are designed to ensure that the individual accessible components work together to create an accessible product. They cover operation, including input and control functions, operation of mechanical mechanisms, and access to visual and audible information. These provisions are structured to allow people with sensory or physical disabilities to locate, identify, and operate input, control and mechanical functions and to access the information provided, including text, static or dynamic images, icons, labels, sounds or incidental operating cues. For example, one provision requires that at least one mode allow operation by people with low vision (visual acuity between 20/70 and 20/200) without relying on audio input since many people with low vision may also have a hearing loss.

Information, Documentation, and Support (Subpart D)

The standards also address access to all information, documentation, and support provided to end users (e.g., Federal employees) of covered technologies. This includes user guides, installation guides for end-user installable devices, and customer support and technical support communications. Such information must be available in alternate formats upon request at no additional charge. Alternate formats or methods of communication, can include Braille, cassette recordings, large print, electronic text, Internet postings, TTY access, and captioning and audio description for video materials.

SECTION 5 - Contract Clauses

FEDERAL ACQUISITION REGULATION (FAR) (48 CFR CHAPTER 1) AND HEALTH AND HUMAN SERVICES ACQUISITION REGULATION CONTRACT CLAUSES

5.1 52.252-2 CLAUSES INCORPORATED BY REFERENCE. (FEB 1998)
This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es): http://www.acquisition.gov/far/ and http://www.hhs.gov/hhsar/

FEDERAL ACQUIISTION REGULATION (FAR) CLAUSES:
52.212-4 COMMERCIAL TERMS AND CONDITIONS (OCT 2018)
52.224-1 PRIVACY ACT NOTIFICATION (APR 1984)
52.224-2 PRIVACY ACT (APR 1984)
52.224-3 PRIVACY TRAINING (APR 1984)
52.239-1 PRIVACY OR SECURITY SAFEGUARDS (AUG 1996)
52.227-14 RIGHTS IN DATA-GENERAL (MAY 2014)

HEALTH AND HUMAN SERVICES ACQUISITION REGULATION CONTRACT CLAUSES:
352.203-70 ANTI-LOBBYING (DEC 2015)
352.208-70 PRINTING AND DUPLICATION (DEC 2015)
352.211-3 PAPERWORK REDUCTION ACT (DEC 2015)
352.224-70 PRIVACY ACT (DEC 2015)
352.224-71 CONFIDENTIAL INFORMATION (DEC 2015)
352.239-73 ELECTRONIC INFORMATION AND TECHNOLOGY ACCESSIBILITY NOTICE (DEC 2015)
352.239-74 ELECTRONIC AND INFORMATION TECHNOLOGY ACCESSIBILITY (DEC 2015)
352.227-70 PUBLICATIONS AND PUBLICITY (DEC 2015)
352.237-74 NONDISCRIMINATION IN SERVICE DELIVERY (DEC 2015)

HHSAR 352.224-71 CONFIDENTIAL INFORMATION (DEC 2015)

(a) Confidential Information, as used in this clause, means information or data of a personal nature about an individual, or proprietary information or data submitted by or pertaining to an institution or organization.

(b) Specific information or categories of information that the Government will furnish to the Contractor, or that the Contractor is expected to generate, which are confidential may be identified elsewhere in this TO. The Contracting Officer may modify this TO to identify Confidential Information from time to time during performance.

(c) Confidential Information or records shall not be disclosed by the Contractor until:

> (1) Written advance notice of at least 45 business days shall be provided to the Contracting Officer of the Contractor's intent to release findings of studies or research, to which an agency response may be appropriate to protect the public interest or that of the agency.

(2) For information provided by or on behalf of the government,

(i) The publication or dissemination of the following types of information are restricted under this TO: Physical location and all descriptions and services of Information Technology implemented, specifically transport and voice services, at these locations.

(ii) The reason(s) for restricting the types of information identified in subparagraph (i) is/are: Public knowledge of such would expose the government to possible physical and cyber-attacks in areas that are critical for emergency public health response efforts.

(iii) Written advance notice of at least 45 business days shall be provided to the Contracting Officer of the Contractor's intent to disseminate or publish information identified in subparagraph (2)(i). The contractor shall not disseminate or publish such information without the written consent of the Contracting Officer.

(d) Whenever the contractor is uncertain with regard to the confidentiality of or a property interest in information under this TO, the contractor should consult with the Contracting Officer prior to any release, disclosure, dissemination, or publication.

FAR 52.212-4 CONTRACT TERMS AND CONDITIONS-COMMERCIAL ITEMS (DEVIATION)

Paragraph (r) of the clause is changed to read as follows:
(r) Compliance with laws unique to Government contracts. The Contractor agrees to comply with 31 U.S.C. 1352 relating to limitations on the use of appropriated funds to influence certain Federal contracts; 18 U.S.C. 431 relating to officials not to benefit; 40 U.S.C. chapter 37, Contract Work Hours and Safety Standards; 41 U.S.C. chapter 87, Kickbacks; 10 U .S.C. 2409 relating to whistleblower protections; 49 U .S .C. 40118, Fly American; and 41 U.S.C. chapter 21 relating to procurement integrity.

FAR 52.212-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS- COMMERCIAL ITEMS (DEVIATION)
The clause is modified to add the following to paragraph (b):
__X__ 52.203-17, Contractor Employee Whistleblower Rights and Requirement To Inform Employees of Whistleblower Rights (April 2014) (41 U .S.C. 4712) relating to whistleblower protections).

52.217-8 OPTION TO EXTEND SERVICES (NOV 1999)
The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 30 days before task order expiration.
(End of clause)

52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)
(a)The Government may extend the term of this contract by written notice to the Contractor within 30 days before or after the contract completion date (defined as the last day the contractor is scheduled to perform); provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 15 days before the contract expires. The preliminary notice does not commit the Government to an extension. If the government exercises an option to extend the term of the contract following the contract completion date, the government is not liable for any costs incurred between contract completion and option exercise. Any services provided during the time between the contract completion date and the option exercise are gratuitous services provided without any expectation of future payment, and the contractor agrees that it will not seek reimbursement for performing such services.
(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.
(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed twelve months.
(End of clause)

FAR 52.252-6 AUTHORIZED DEVIATIONS IN CLAUSES (APR 1984)
(a) The use in this solicitation or contract of any Federal Acquisition Regulation (48 CFR Chapter 1) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the date of the clause.

(b) The use in this solicitation or contract of any Health and Human Services Acquisition Regulations (48 CFR Chapter 3) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the name of the regulation

SECTION 6 - Instructions, Conditions, and Notices to Quoters or Respondents

This is a notice that this order is a COVID 19, FAR 6.302-2 Unusual and Compelling Urgency requirement under FAR Part 12 and 13, authorized by the HHS COVID-19 CLASS J&A. This urgent requirement is being competed rapidly and is set aside for Women Owned Small Business.

6.1 SOLICITATION PROVISIONS INCORPORATED BY REFERENCE (FAR 52.252-1, FEBRUARY 1998)

This solicitation incorporates one or more solicitation provisions by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. The quoter is cautioned that the listed provisions may include blocks that must be completed by the quoter and submitted with its quotation or offer. In lieu of submitting the full text of those provisions, the quoter may identify the provision by paragraph identifier and provide the appropriate information with its quotation or offer. Also, the full text of a solicitation provision may be accessed electronically at this/these address(es): http://www.acquisition.gov/far/ and http://www.hhs.gov/hhsar/

FEDERAL ACQUISITION REGULATION (FAR) PROVISIONS

FAR 52.212-1 Instructions to Offerors – Commercial Items (June 2008)

HHS ACQUISITION REGULATION (HHSAR) (48 CFR CHAPTER 3) PROVISIONS

HHSAR 352.239.73 Electronic Information and Technology Accessibility Notice (Dec 2015)

HHSAR 352.239-73(a) Electronic and Information Technology Accessibility (January 2010)

(a) Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998, and the Architectural and Transportation Barriers Compliance Board Electronic and Information (EIT) Accessibility Standards (36 CFR Part 1194), require that, unless an exception applies, all EIT products and services developed, acquired, maintained, or used by any federal department or agency permit-

> (1) Federal employees with disabilities to have access to and use information and data that is comparable to the access and use of information and data by federal employees who are not individuals with disabilities; and
>
> (2) Members of the public with disabilities seeking information or services from a federal agency to have access to and use of information and data that is comparable to the access and use of information and data by members of the public who are not individuals with disabilities.

(b) Accordingly, any vendor submitting a proposal/quotation/bid in response to this solicitation must demonstrate compliance with the established EIT accessibility standards. Information about Section 508 is available at http://www.section508.gov/. The complete text of Section 508 Final Provisions can be accessed at http://www.access-board.gov/sec508/standards.htm.

(c) The Section 508 accessibility standards applicable to this solicitation are identified in the Statement of Work/Specification/Performance Work Statement. In order to facilitate the Government's evaluation

to determine whether EIT products and services proposed meet applicable Section 508 accessibility standards, offerors must prepare an HHS Section 508 Product Assessment Template, in accordance with its completion instructions, and provide a binding statement of conformance. The purpose of the template is to assist HHS acquisition and program officials in determining that EIT products and services proposed support applicable Section 508 accessibility standards. The template allows vendors or developers to self-evaluate their products or services and document in detail how they do or do not conform to a specific Section 508 accessibility standard. Instructions for preparing the HHS Section 508 Evaluation Template may be found under Section 508 policy on the HHS Office on Disability website (http://www.hhs.gov/od/).

(d) Respondents to this solicitation must also provide any additional detailed information necessary for determining applicable Section 508 accessibility standards conformance, as well as for documenting EIT products or services that are incidental to the project, which would constitute an exception to Section 508 requirements. If a vendor claims its products or services, including EIT deliverables such as electronic documents and reports, meet applicable Section 508 accessibility standards in its completed HHS Section 508 Product Assessment Template, and it is later determined by the Government - i.e., after award of a contract/order, that products or services delivered do not conform to the described accessibility standards in the Product Assessment Template, remediation of the products or services to the level of conformance specified in the vendor's Product Assessment Template will be the responsibility of the Contractor and at its expense.

6.2 GENERAL INFORMATION

The Government's response to the inquiries will be directly emailed to the vendor(s). Any resulting additions, deletions or changes to the solicitation will be made by issuance of a formal amendment. Quoters are instructed specifically to contact only the issuing contract office in connection with any aspect of this requirement prior to contract award. The Government does not intend to extend the due date for quotes.

Given this is an urgent and compelling, COVID-19 requirement, the Government will not be able to respond to questions received in regard to the requirement.

The quote must be submitted no later than **Friday, September 25, 2020 at 5:00 pm Eastern Time**. Quotes must be directly emailed to the Contracting Officer, Jennifer Browning, via email at Jennifer.browning@hhs.gov and to the Contract Specialist, Lashawn Haggins, at Lashawn.haggins@psc.hhs.gov.

It is anticipated that a firm fixed price type order will be placed. Any exceptions must be stated by the quoter. The NAICS Code for this requirement is 541380.

Quoters are therefore reminded that they are to submit offers in response to this solicitation that will be binding should the Government select them for award without discussions, and to do so that they must include their best firm-fixed pricing on a fully complete SF1449 and signature by the responsible individual on the face page of the SF1449. Failure to do so may result in the quoter being determined as non-responsive and not considered for award.

Your attention is directed to the requirements for technical and business proposals to be submitted in accordance with the following instructions establishing the acceptable minimum requirements for the content of proposals. Failure to comply with the Instructions to quoters may result in the quoter being determined as non-responsive and not considered for award. The RFQ does not commit the Government to pay any costs for preparation and submission of a proposal. In addition, the Contracting Officer is the only individual who can legally commit the Government to the expenditure of public funds in connection with this proposed acquisition. If a quoter has activity to report, it shall complete SF-LLL "Disclosure of Lobbying Activities" and shall include one signed copy with the business proposal.

The proposal shall be prepared and submitted in two volumes: Volume I - Technical Proposal and Volume II- Business Proposal. Each of these volumes shall be separate and complete in itself so that evaluation of one may be accomplished independently of evaluation of the other. The Government shall evaluate proposals in accordance with the Evaluation Criteria. It is essential that the Quoter explicitly address all evaluation criteria including subjective factors in the written proposal.

SUBMISSION INDICATES ACKNOWLEDGEMENT OF REPRESENTATIONS, CERTIFICATIONS
Quoters are to include a completed copy of the provision at FAR 52.212-3, Offeror Representations and Certifications – Commercial Items (Oct 2018) with its offer or acknowledge its listing in the System for Award Management (SAM) website.

6.3. VOLUME I – TECHNICAL PROPOSAL INSTRUCTIONS - Limited to no more than 3 pages (page limit does not include VPAT).

Quoters shall provide sufficient information to evaluate the technical solution and proposed personnel to complete the order. The technical proposal shall discuss the proposed technical approach in sufficient detail to clearly and concisely demonstrate that the Quoter has an understanding of all requirements specified in the requirement Description/Performance Work Statement.

If applicable, the technical proposal shall include a list of names, labor categories and proposed duties of the key personnel assigned to this order. Their resumes are not necessary at this time but must be provided at the Contracting Officer's Representative's request and shall at a minimum include information on education, background, recent experience, and specific scientific or technical accomplishments and experience which relates to the requirements of this RFQ. Also, the technical proposal shall designate a responsible technical official who can commit the firm on technical issues and directions with the current scope of work.

Provide an Accessibility Conformance Report (ACR) for each commercially available Information and Communication Technology (ICT) item offered through this contract. Create the ACR using the Voluntary Product Accessibility Template Version 2.1 or later, located at https://www.itic.org/policy/accessibility/vpat. Complete each ACR in accordance with the instructions provided in the VPAT template. Each ACR must address the applicable Section 508 requirements referenced in the Work Statement. Each ACR shall state exactly how the ICT meets the applicable standards in the remarks/explanations column, or through additional narrative. All "Not Applicable" (N/A) responses must be explained in the remarks/explanations column or through additional

narrative. Address each standard individually and with specificity, and clarify whether conformance is achieved throughout the entire ICT Item (for example - user functionality, administrator functionality, and reporting), or only in limited areas of the ICT Item. Provide a description of the evaluation methods used to support Section 508 conformance claims. The agency reserves the right, prior to making an award decision, to perform testing on some or all of the quoter's proposed ICT items to validate Section 508 conformance claims made in the ACR. Describe your approach to incorporating universal design principles to ensure ICT products or services are designed to support disabled users. Describe plans for features that do not fully conform to the Section 508 Standards. Describe "typical" user scenarios and tasks, including individuals with disabilities, to ensure fair and accurate accessibility testing of the ICT product or service being offered.

6.4. VOLUME II – PRICE PROPOSAL INSTRUCTIONS

Quoter shall submit a pricing table using the format in section 1.4 and include a detailed breakdown identifying what is included, show the proposed discounts for the rate, and the rate proposed for the particular labor category inclusive of the discount.

SECTION 7 – EVALUATION CRIERIA AND FACTORS FOR AWARD

7.1. EVALUATION

The evaluation shall be conducted in accordance with the evaluation criteria stated below. Therefore, each initial quote should contain the quoter's best terms and conditions. The Government has the right to award without discussions. The evaluation criteria are as follows:

Factor 1: Technical Acceptability
Factor 2: Price

7.2. BASIS FOR AWARD

The following factors will be considered in evaluating proposals: technical acceptability and price. Award will be awarded based on technical acceptability and the overall best value to the Government. The Government will base the award decision off of the quoter evaluated to provide the overall best value to the Government. Best value will be determined by the Government as the quoter evaluated as providing the lowest price, technically acceptable proposal in accordance with this solicitation.

The Government will evaluate price quotes, not only to determine whether they are fair and reasonable, but also to determine Quoter understands the requirements, and ability to meet all requirements and scope.

The Contracting Officer reserves the right to review of past performance information from the federal system to what he/she has been determined to be relevant to determine contractor responsibility for award. The Government reserves the right to reject any quote that includes any assumption(s) that impact satisfying the Government's requirements.

7.3. TECHNICAL EVALUATION CRITERIA:

Factor 1: Technical Acceptability
The following will be used to determine Technical Acceptability:

1) Includes all services and minimum requirements listed in this RFQ;
2) Prices the services in this RFQ;
3) Proposes services that fulfill the entire requirement described in this RFQ;
4) Contractor must demonstrate and certify that it meets the following minimum requirements:
    a. Contractor has the capacity to perform wastewater testing for SARS-CoV-2 and associated Quality Assurance/Quality Control (QA/QC) required for on a maximum of 200 samples per week for 8 weeks in Phase 1 and up to 640 samples per week for 9 weeks in optional Phase 2.
    b. Contractor can consistently report results of wastewater surveillance testing within 36 hours of sample collection for the duration of this Contract.
    c. Contractor can specify appropriate QA/QC measures and document their implementation as a part of their wastewater analysis methodology.
    d. Contractor has the demonstrated capacity to independently forge partnerships with local officials, including but not limited to local water/sewer departments.
    e. Contractor has previous experience performing wastewater testing activities with appropriate QA/QC to maintain the uncorrupted nature of the raw and modeled data required, including but not limited to, protocol of laboratory methods utilized, human fecal normalization parameter, inhibition evaluation, standard curves (RT-qPCR), extraction blanks, and no template controls..
    f. Contactor can secure all equipment necessary to perform the services required under this Contract.
    g. Contractor has all appropriate licenses or waivers in place to perform all wastewater testing services.
    h. Contractor runs laboratory analysis, isolating the genetic material (RNA) of SARS-CoV-2 and analyzing and testing to quantify the amount of SARS-CoV-2 RNA molecular targets via reverse transcriptase quantitative polymerase chain reaction or droplet digital RT-PCR.
    i. Contractor uses computational biology models to identify strains circulating in the state, and to estimate COVID-19 cases

Factor 2: Price

This factor addresses the quoter's price. All quoter's submissions shall incorporate all item(s) that will be applied to this contract. The total price, inclusive of all options, will be evaluated to determine reasonableness and realism. As part of the price analysis, the government will consider whether the proposed labor mix, level of effort and materials are consistent with the Technical Volume. If the Technical Volume and pricing are inconsistent, the quoter may be ineligible for award.

Organizational Conflict of Interest

If the Government determines that an organizational conflict of interest (OCI) exists, that cannot be satisfactorily avoided, neutralized or mitigated or waived, the Contracting Officer may determine that the quoter will not be eligible for award. The Government reserves the right to only consider mitigation plans proposed by the apparent successful quoter.