OFFICE OF THE ASSOCIATE DIRECTOR FOR COMMUNICATION

Request for Quote (RFQ) Form

For Ordering Off OADC Communication Services BPA

Part 3. Performance Work Statement

I. Background and Need:

The Office of the Associate Director for Communication (OADC), Division of Public Affairs (DPA) is charged with oversight and execution of public affairs, news and digital media, and external and employee relations throughout CDC.

DPA's **mission** is to combine media relations, digital communication, issues management, social responsibility, information dissemination, strategic communication, and internal and external stakeholder engagement to advance achievement of public health goals and understanding of critical health issues facing the public.

DPA's national vision is to ensure everyone has clear, concise, and crucial information to protect their health.

DPA's strategic goals are to

- Advance CDC as a leader and innovator in public affairs
- Ensure CDC's voice is consistent, trusted, and heard
- Engage CDC's communicators by offering valued tools, expertise, and services
- Build and maintain an environment within DPA that promotes mutual respect and collaboration

Within the Division of Public Affairs, the News Media Branch (NMB) develops and implements comprehensive, integrated media strategies to target audiences through media (e.g. broadcast, print, and digital). NMB works collaboratively across the Agency to provide media support and consultation, online media monitoring, digitally integrated press release dissemination, media materials development, and proactive and reactive media plans and strategies that leverage available traditional and digital media channels to best deliver CDC's messages. NMB also provides spokesperson and other media relations training and technical assistance to CDC staff. NMB coordinates with HHS ASPA on behalf the Agency on CDC media relations activities. Having a comprehensive, integrated, and strategic media relations programs is integral to achieving CDC's overall communication objectives and in ensuring a coordinated, cohesive Agency media response to critical and emerging public health initiatives and priorities.

The contractor shall provide expert technical services in media relations in support of the

Division of Public Affairs, News Media Branch goals and objectives. All work shall adhere to established CDC and HHS and s policies, including public affairs/media, clearance, security, and privacy policies.

II. Project Objective:

The objective of this contract is to support the News Media Branch's media relations activities.

III. Description of Work

All services shall be performed in accordance with the performance period stated in this acquisition. Please note that due to the nature of the CDC's work, the contractor may have access to sensitive unclassified, classified, and/or confidential information. Therefore, the contractor must maintain a high level of confidentially to protect governmental information. The contractor cannot share or disseminate any governmental information to internal or external parties without the Agency's consent and authorization. The contractor is required to perform the following:

Task 1: Management and Administration

Objective: The contractor shall designate a project manager (PM) for the entire period of performance to monitor all contract service activity, ensure quality of all deliverables, control contract costs, and supervise contractor employee(s) to complete all services required in this Statement of Work (SOW).

The PM shall serve as one of the principal points of contact with the government. The PM shall:

- Participate in the Post-Award Meeting:
    - The contractor shall plan and schedule a Kick-off Meeting with the Contracting Officer's Representative (COR), the CDC Contracting Officer (CO), the CDC Contracting Specialist (CS), the lead project officer, and other NMB staff.
    - The contractor will collaborate with the COR on the agenda and provide the final agenda to the COR and the lead project officer (PO) no later than (NLT) two (2) business days before the meeting. The contractor shall provide the minutes NLT three (3) business days after the meeting to the COR.
- Attend the COR Monthly Touchpoint Teleconference calls and provide the minutes from each session
- Provide a final project management plan to the COR for approval within ten (10) business days after the Kick-off Meeting
- Supervise all contractor employees

- Ensure and monitor the quality of all work products
- Provide staffing levels that allow for transparent continuity of services
- Maintain close communication with the COR and the lead NMB Project Manager:
    - The contractor shall update the COR and the lead project officer on project status through weekly, bi-weekly, and/or monthly teleconferences. The contractor will also communicate with the COR through email and phone as need to make sure the work proceeds according to the established due date.
- Prepare and disseminate monthly and annual reports
- Schedule and attend weekly meetings and/or conference calls for the first two months and biweekly thereafter to discuss and review completed work, work in progress, quality control issues, timelines, and other business concerns
- Resolve customer service complaints within 3-5 business days.
- Resolve contractor performance issues within 30-60 days after notification from the COR
- Collaborate with the contractor's senior communications specialist to develop and maintain a project tracker report approved by the COR. Disseminate the project tracker report weekly to the COR, lead project officer, and other NMB staff on Fridays NLT 3:00 p.m.

Task 2: Strategic Media Relations Support

Objective: As part of OADC's overall communication activities, the contractor shall participate in setting media strategies for CDC and CDC leadership. The contractor shall made recommendations and develop media strategies on a variety of media issues and topics. The contractor shall designate a senior media strategist for the entire period of performance to provide expert technical strategic services in media relations.

The senior media strategist shall serve as a media relations expert. The senior media strategist shall:

- Provide analysis of existing or emerging public health issues and priorities and provide recommendations for proactive and reactive media approaches using available media tools and systems.
- Use available media tools and systems to create proactive media outlet engagement strategies.
- Collaborate extensively with staff within the Office of the Associate Director for Communication and other key individuals and offices across the Agency to ensure media strategy and messages are aligned with

Division, OADC, and Agency goals and objectives; maintain updated documentation and disseminate to inform strategic media planning

- Stay current on public health issues that may be relevant to specific work assignments by conducting environmental and media scans as needed across traditional and digital media channels
- Coordinate media interviews in coordination with NMB FTE staff, CDC subject matter experts and Agency communication staff.
- Implement media relations strategies and activities related to current CDC priority initiatives, as indicated.
- Ensure media materials and products are reviewed by DPA, OADC, and other internal stakeholders as warranted per internal polices and processes.
- Ensure work products are completed timely and delivered to the agency by the due date
- Prepare for and attend strategic communication meetings with NMB leadership, Agency spokespersons, or others as requested
- Collaborate with the contractor's PM to develop and maintain a project tracker report approved by the COR. Ensure the contractor's PM captures all completed and active work assignments in the report NLT 2:00 pm each Friday

Task 3: Media Technical Writing Support

Objective: As part of OADC's overall communication activities, the contractor shall participate in develop media products including talking points and press releases for a variety of CDC topics. The contractor shall designate a senior technical writer for the entire period of performance to provide expert technical writing services for media relations.

- Translate complex CDC data and scientific content into key messages for Agency-level spokesperson use across digital and traditional media channels
- Recommend, develop, and write a variety of media products, including but not limited to
    - telebriefing and press conference scripts and talking points;
    - reactive statements;
    - press releases;
    - key messages;
    - op-ed pieces and other opinion commentary;
    - speeches/presentations that may generate media interest;
    - other media content and materials
- Review media products (as listed above) and provide recommendations to improve readability; edits for clarity; and recommendations on message framing to NMB chief and senior press officers as part of NMB quality assurance process.
- Ensure plain language and HHS/CDC clear communication principles and assessment tools are used in and applied to all media materials.

- Ensure highly technical scientific papers, including CDC Morbidity and Mortality Week Reports and other scientific publications, reports, guides, and articles are translated into content that is suitable for media (traditional and digital).
- Ensure media materials and products are reviewed by DPA, OADC, and other internal stakeholders as warranted per internal polices and processes.
- Ensure work products are completed timely and delivered to the agency by the due date
- Prepare for and attend strategic communication meetings with NMB leadership, Agency spokespersons, or others as requested
- Collaborate with the contractor's PM to develop and maintain a project tracker report approved by the COR. Ensure the contractor's PM captures all completed and active work assignments in the report NLT 2:00 pm each Friday

Task 4: Media Monitoring and Analysis

Objective: The contractor shall provide media monitoring summaries for the entire period of performance.

- Provide a plan for media monitoring ("clips"). The plan should outline strategies to ensure seamless cutover from previous media monitoring methods to avoid break in service.
- Consistent with CDC's existing media monitoring ("clips") service for priority Agency topics, develop daily, weekly, monthly and/or quarterly news media summaries, as per approved plan, for distribution via email among internal CDC audiences, which may model current CDC media monitoring report format and frequency:
    - Daily News Clips – Customized daily report sent via email to internal distribution list. Includes links around priority CDC topics.
    - Today's News – Daily compilation of the full text of articles with significant CDC mentions. Approximately 30-70 articles include per day. Includes full-text versions of articles. In addition to distributing as an email, also send Word document, transmitted by FTP file, for use on CDC intranet.
    - Breaking News – sent via email, including nights and weekends. CDC-related news stories, from major news outlets. Five – 10 stories per day on average.
- Maintain media monitoring email lists and upon COR approval, add and delete recipients; work collaboratively with COR and NMB staff to ensure list is reviewed and updated at least once per year.
- Upon request, provide media monitoring summaries ("clips") for CDC programs on specific topics.

- Provide at least one annual media monitoring report and analysis, reviewing and applying content analysis and other study methodologies to determine placement, reach, and impact of CDC's media efforts on priority CDC public health topics.
- Ensure media materials and products are reviewed by DPA, OADC, and other internal stakeholders as warranted per internal polices and processes.
- Ensure work products are completed timely and delivered to the agency by the due date
- Prepare for and attend strategic communication meetings with NMB leadership, Agency spokespersons, or others as requested
- Collaborate with the contractor's PM to develop and maintain a project tracker report approved by the COR. Ensure the contractor's PM captures all completed and active work assignments in the report NLT 2:00 pm each Friday

Task 5: Media/Spokesperson Training

Objective: The contractor shall provide executive/c-suite-level media/spokesperson training for CDC senior leaders and select subject matter experts the entire period of performance.

- Develop a media/spokesperson training plan that outlines proposed approach to media/spokesperson training. The plan should describe an approach for individual assessment, training, coaching, and follow-up for CDC senior leaders and subject matter experts to prepare them for print, broadcast, and other media opportunities.
- Upon approval of the plan, and in collaboration with OADC/DPA/NMB leadership, conduct up to 6 one-on-one or group training sessions per year for CDC senior leadership and subject matter experts, in person at CDC's main campus or remotely for non-Atlanta based staff.
- Use existing CDC priorities, messages, and materials to inform media training.
- Ensure that best practices for executive-level risk communication, crisis communication, and media relations are incorporated into all aspects of training.
- Ensure media materials and products are reviewed by DPA, OADC, and other internal stakeholders as warranted per internal polices and processes.
- Ensure work products are completed timely and delivered to the agency by the due date
- Prepare for and attend strategic communication meetings with NMB leadership, Agency spokespersons, or others as requested
- Collaborate with the contractor's PM to develop and maintain a project tracker report approved by the COR. Ensure the contractor's PM captures all completed and active work assignments in the report NLT 2:00 pm each Friday

The contractor may be required to provide additional surge support for surge media support,

technical writing, and/or for 24/7 media monitoring (e.g. for public health responses). Surge support may be required due to developments impacting the need for support services including Emergency Operations Center activation and associated impact on application requirements or performance, reorganization, the end of the Fiscal Year, or similar events that increase the required level of effort, urgency or time pressure to getting a task or subtask accomplished. The surge support requirement is included as separate line items associated with each performance period, for the base and options; see the line item schedule. The surge activities will be separately priced for labor hours.

IV. DELIVERABLES/REPORTING SCHEDULE

Post-Award Kick-off Meeting: Within ten (10) calendar days after contract award, the contractor shall participate in a Post-Award Kick-off meeting for at least two (2) hours with NMB Leadership, the COR, lead project officer, technical monitors, and/or the Office of Acquisition Services' Contracting Officer and Contract Specialist (CO/CS). The contractor will collaborate with the COR on the agenda and provide the final agenda to the COR and lead project officer (PO) no later than (NLT) two (2) business days before the meeting. The contractor shall provide the minutes NLT three (3) business days after the meeting to the COR.

COR Monthly Touchpoint Teleconference Calls: The contractor shall attend a monthly teleconference with the COR. This is a non-programmatic discussion that will allow the contractor to provide status updates to the COR and to address any matters of concern. The contractor shall provide the meeting agenda to the COR within two (2) business days prior to the meeting. After the meeting, the contractor will provide a high-level summary of the discussion and any action items within three (3) business days to the COR. The COR reserves the right to decrease the frequency of the Touchpoint Teleconference calls.

Project Plan: The contractor shall provide the COR and the lead project officer with a project plan within ten (10) business days after the Post-Award Kick-off Meeting. The contractor may be required to revise the project plan to obtain COR approval. The contractor must execute the final plan after COR approval. The project plan must include the contractor's:

- Project management approach for performing the services listed in the SOW
- Change Management Plan to describe a change control process for submitting draft and final communication materials and speeches to the agency for review and approval
- Communications Management Plan that describes what, how, and when information will be shared and distributed to ensure project success
- Quality Management Plan that describes how quality management will be used to

ensure that the deliverables for the project meet established standards of acceptance

- Risk Management Plan that describes the approach to identify and manage risks associated with the project
- Escalation Policy/Procedure to address customer service problems identified by contractor or COR
- Staffing Management Plan that discusses a plan to maintain acceptable staffing levels with subject matter experts during core and non-core hours; time allocation of each staff; process to address and resolve customer service complaints and performance issues; and a protocol to replace staff in the event of unacceptable performance

Monitoring Reports: The contractor shall deliver monthly status and annual reports to the COR and/or the OAS CO/CS within the time specified below via E-mail.

A. **Monthly Status Report**: The contractor shall provide the government with a monthly status report that includes a written narrative to the COR and/or CO/CS with the following information:
    - Status of current tasks, including a summary of progress toward completion of each work activity
    - Status of any incomplete tasks
    - Problems/barriers to progress, including any anticipated issues going forward, and the contractor's assessment of specific impact of such problems on estimated costs and how barriers were addressed

B. **Annual Report:** The contractor shall provide the government with a report summarizing all contract activities at the conclusion of the base year and each option period (if exercised). This report shall include additional information such as:
    - Yearly workload data, including summary of overall hours worked on the contract subdivided by task
    - Financial data and standing in relation to submitted invoices and payments received on the contract (e.g., table showing overall billed amount and overall received payments by CLIN and fiscal year for the period of performance)

DELIVERABLES AND SCHEDULE				
Task	**Description**	**QTY/Mode**	**Due Date**	**Deliver**
1/2	Post-Award Kick-off Meeting	1/In-Person	Within 10 business days after contract	COR/PO
1	Final Approved Agenda: Post-Award Kick-off Meeting (PAM) & COR	1 – PAM; 12 – CMT/MS Word or PDF via E-mail	NLT two (2) days before each meeting	COR/PO
1	Minutes/Notes: PAM & CMT	1 – PAM; 12 - CMT/MS Word or PDF via E-mail	NLT three (3) business days after the meeting	COR/PO
1	Project Management Plan	1/MS Word or PDF via E-mail	Within 5 business days after the Post-Award Kick-Off Meeting	COR/PO
1/2	COR Monthly Touchpoint Teleconference Calls	12 per each period of performance/Conference Call	Monthly NLT 15th of each month	COR
1/2	Weekly Strategy Meetings & Conference Calls	In-Person	Weekly or Bi-Weekly as requested by the Agency	COR/DPA Team
2	Strategic Media Relations Work Products (Drafts)	1 Copy per each work product/MS Word, PDF, or PowerPoint as requested by the agency via E-mail	As requested by the agency per the due date on the Tracker Report	COR/DPA Team
2	Strategic Media Relations Work Products (Final)	1 Copy per each work product/MS Word, PDF, or PowerPoint as requested by the agency via E-mail	As requested by the agency per the due date on the Tracker Report	COR/DPA Team
3	Technical Writing Work Products (Drafts)	1 Copy per each work product/MS Word, PDF, or PowerPoint as requested by the agency via E-mail	As requested by the agency per the due date on the Tracker Report	COR/DPA Team

3	Technical Writing Work Products (Final)	1 Copy per each work product/MS Word, PDF, or PowerPoint as requested by the agency via E-mail	As requested by the agency per the due date on the Tracker Report	COR/DP A Team
1	Monthly Status Report	1/MS Word or PDF via E-mail	Monthly NLT 5th day of each month	COR/PO
1	Annual Report	1 per each period of performance/MS Word with MS Excel via Email	Due 30 days after expiration of the period of performance; period (if exercised)	COR/PO
4	Media Monitoring and Analysis Plan	1 MS/Word or PDF via email	Within 5 business days after the Post-Award Kick-Off Meeting	COR/PO
4	Media Monitoring Delivery	To approved internal CDC email list and times as per requirements as outlined in Task 4.4	Within 2 business days of approval of media monitoring plan	Approve d email distributi on list
4	Annual Media Monitoring Report and Analysis	1 per each period of performance/MS Word with MS Excel via Email	Due 30 days after established time frame for analysis	COR/PO
5	Media Spokesperson Training Plan, including resumes or bio sketches of proposed trainers.	1 MS/Word or PDF via email	Within 10 business days after the Post-Award Kick-Off Meeting COR/PO	COR/PO
5	Media Spokesperson Trainings	Up to 6 one-on-one or group trainings per year	To be determined based on need and approved plan	COR/PO

All task order deliverables intended for communication to the public must comply with Public Law 111–274, the Plain Writing Act of 2010. For Plain Language information and the Federal Plain Language Guidelines see www.plainlanguage.gov.

All materials will be submitted electronically in MS compatible format that meets CDC standards and is readily available at CDC (e.g. MS Office (Word, Excel, PowerPoint) or Adobe Acrobat. All reporting requirements and written deliverables as part of this contract

will be supplied to the project Contracting Officer Representative (COR). Acceptance of any written deliverables is pending CDC COR review and correction to any resulting comments, to be confirmed in writing and documented in the closest following monthly report. Any schedule of interim deliverables may be revised according to CDC acceptance of an updated written work plan by the COR during the project with the restriction that these changes must not impact the overall period of performance, scope, or specifications of the award, or otherwise impinge on the authority of the contracting officer. It is the responsibility of the contractor to fully understand what changes require contracting officer approval.

V. Performance Matrix

The Performance Matrix (Quality Assurance Surveillance Plan) is the portion of the performance-based SOW that explains the Agency's expectations and how deliverables or services will be monitored and evaluated.

Work Requirement	Acceptable Quality Level (AQL)	Monitoring Method	Incentives/ Disincentives
Task 1 Management & Adminstration	• Occurs at regularly scheduled times • Contractor is prepared to discuss relevant project issues, is responsive to project planning issues/project improvments, and documents meetings as described in PWS (may be corrected to COR comments) • Quality management plan is adhered to 95% of the time. • Sufficient resource utilization of contractor employees to ensure project success; 95% effectiveness of project plan; 98% customer and stakeholder satisfaction	• 100% review (by the COR) • Unacceptable meetings will be documented as customer complaints, contractor may be allowed to correct any insufficiences to CDC satisfaction	• Contractor's performance is documented as past performance using CPARS which is considered for future awards. • `Performance is considered in determining whether to exercise the option periods • Repeated complaints on different events/tasks but the same issue will be elevated for higher level

Work Requirement	Acceptable Quality Level (AQL)	Monitoring Method	Incentives/ Disincentives
Task 2 & 3 Strategic Media relations support & Technical Writing	95% of ALL products submitted by the established due date 95% of ALL products adhere to standard grammatical, style, and writing best practices and guidelines ALL deliverables must encompass all QA standards, Accessibility, 508 compliance checks, conformance with Federal Plain Language Guidelines, and adherence to CDC policies, guidelines, standards, and best practices % of CDC's feedback on draft content is reflected in the final product/material At least 95% of media messaging is appropriate for the subject and audience At least 95% of media messaging resonates with the CDC spokesperson's voice and/or CDC's core messages	• COR Random sampling • 100% review by the DPA Team • Unacceptable quarterly conference meetings will be documented as customer complaints, contractor may be allowed to correct any insufficiences to CDC satisfaction	resolution (senior management and/or OAS)
Task 4 Media Monitoring and Analysis	95% of relevant media articles are sent to CDC within established timelines 90% of media articles match CDC topics of interest.	• COR Random sampling • 100% review by the DPA Team • Unacceptable quarterly conference meetings will be documented as customer complaints, contractor may be allowed to correct any insufficiences to CDC satisfaction	
Task 5 Media/Spokespersons Training	95% of media training resonates with the CDC spokesperson's voice and/or CDC's core messages 95% of training occurs on time	• COR and NMB observation of training events • 100% COR review of training plan	

Work Requirement	Acceptable Quality Level (AQL)	Monitoring Method	Incentives/ Disincentives
	Training plan reflects CDC media policy and media relations best practices		

VI. Period of Performance:

The Period of Performance is:

Year 1 (Basic Period): 6/15/2020-6/14/2021

Year 2 (Option): 6/15/2021-6/14/2022

Year 3 (Option): 6/15/2022-6/14/2023

Year 4 (Option): 6/15/2023-6/14/2024

Year 5 (Option): 6/15/2024-6/14/2025

VII. Place of Performance

The contractor shall perform Task 2 and 3 (senior media strategist and technical writer) at the CDC Roybal Campus facility located in Atlanta, Georgia. Regarding Task 5 (media/spokesperson training) all trainings will be conducted at CDC's main campus unless otherwise specified by the COR. All other tasks can be performed offsite at the contractor's facility with the expectation the COR and the CDC/ATSDR Director (or other agency leaders) may require the contractor's project manager to regularly visit the CDC headquarter facility in Atlanta, Georgia.

Core and Non-Core Hours Requirement: The Contractor's core hours of operations shall start between 7:00 am and 9:00 am and end between 3:30 pm and 5:30 pm Eastern Standard Time, Monday through Friday, excluding Federal holidays and emergency closures. Additionally, the contractor must have the capacity to perform Task 2, and Task 3, and Task 4 during non-core hours in the event of a public health emergency or another external event that would require CDC to be activated beyond core hours.

Telework Eligibility: The requirements for Task 2 and 3 and the performance thereof may be achieved through situational telework. If the contractor proposes telework for the senior

media strategist and technical writer, the contractor's employee must work onsite for the initial six (6) months. Thereafter, the COR will determine telework eligibility based upon successful performance of the service. The COR, at any time, may cancel a telework agreement to support the agency's needs and requirements.

Travel. The contractor's strategic media relations and technical writing support specialists may be required to travel to local (metropolitan Atlanta) events, as well as to other CDC Atlanta campuses. support for task 5 may require up to 6 trips per year to Atlanta.

All travel must be authorized by the COR and be in compliance with the task order and all other applicable requirements.

Prior approval: Requests for travel approval shall:

- Be prepared in a legible manner
- Include a description of the purpose of the trip
- Be summarized by traveler
- Identify the task order number
- Identify the task order CLIN
- Be submitted in advance of the travel with sufficient time to permit review and approval

The contractor shall use only the minimum number of travelers and rental cars needed to accomplish the trip purpose. Travel shall be scheduled during normal duty hours whenever possible. Airfare will be reimbursed for actual common carrier fares which are obtained by the most reasonable and economical means. The contractor shall provide a Trip Report for each trip associated with a travel approval. The contractor shall maintain a summary of all approved travel, to include at a minimum, the name of the traveler, location of travel, duration of trip, total cost of trip. In the event of local travel, the contractor must provide prior notification to the COR. The contractor is responsible for making all travel arrangements.

The agency will reimburse the contractor for local travel-related expenses up to the maximum allowable amount in accordance with Federal Travel Regulations. The contractor must provide an itemized report that details all travel-related expenses (local mileage and/or public transportation only), including the submission of copies of receipts and other supporting documents. The agency will not reimburse the contractor for any food expenses.

VIII. Government Furnished Materials, Facilities and Property

CDC will provide Strategic Media Support and Technical Writer contractor personnel with adequate work space in an office environment typically provided to Government personnel that includes materiel equivalent to that used by the Government personnel,

such as personal commuter, desk, chair, cabinet space, telephone, FAX, commuters with access to the Internet and local area network (LAN) and similar items. Badge and keys will also be provided as appropriate. All such items utilized by the contractor remain the property of the Government.

If performance of this contract is within and on Government facilities, and the Government-furnished property or contractor-acquired property is for use only within or on the Government facilities, the control and accountable record keeping for such property shall be retained by the Government (see FAR 52.245-1, Property Records). The Contractor shall remain accountable for loss or damage but will not be required to submit an annual inventory or place its own bar codes on the items. The Government will provide property labels and other identification for contractor acquired Government property under this paragraph. CDC will provide the contractor access to necessary files and team document storing and sharing tools (e.g., SharePoint).

IX. Information Security and Privacy 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) employee 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. Protect 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:	[X] Low [ ] 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

4) **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 [ ] Moderate [ ] High

5) **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*.

6) **Protection of Sensitive Information**. For security purposes, information is *or* may be sensitive because it requires security to protect its confidentiality, integrity, and/or availability. The Contractor (and/or any subcontractor) shall protect 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.

7) **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 and CDC policies. Unauthorized disclosure of information will be subject to the HHS/CDC 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).

8) **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)*. .

9) **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 protect against attacks that attempt to downgrade connections to plain HTTP. For internal-facing websites, the HTTPS is not required, but it is highly recommended.

10) **Contract Documentation**. The Contractor shall use provided templates, policies, forms and other agency documents to comply with contract deliverables as appropriate.

11) **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 and CDC-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 *[CDC-provided delivery date]*.

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 CDC Office of Chief Information Security Officer (OCISO).

12) **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 CDC 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.

13) **Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA)** – The Contractor shall assist the CDC Senior Official for Privacy (SOP) or designee with conducting a PTA for the information system and/or information handled under this contract in accordance with HHS policy and OMB M-03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.

    a. The Contractor shall assist the CDC 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 CDC SOP that a review is required based on a major change to the system (e.g., new uses of information collected, changes to the way information is shared or disclosed and for what purpose, or when new types of PII are collected that could introduce new or increased privacy risks), whichever comes first.

A. 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/CDC 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 *CDC Security Awareness Training (SAT)* 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 (RBT) ***within 60 days*** of assuming their new responsibilities. Thereafter, they shall complete RBT at least ***annually*** in accordance with HHS policy and the *HHS Role-Based Training (RBT) of Personnel with Significant Security Responsibilities Memorandum.*

   All HHS employees and contractors with SSR who ***have not*** completed the required training within the mandated timeframes shall have their user accounts disabled until they have met their RBT requirement.

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.

B. 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 *CDC 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.

C. Incident Response

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.

OMB Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information" (03 January 2017) states:

> **Definition of an Incident:**
> *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.*
> **Definition** of a **Breach:**

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.

It further adds:

> A breach is not limited to an occurrence where a person other than an authorized user potentially accesses PU by means of a network intrusion, a targeted attack that exploits website vulnerabilities, or an attack executed through an email message or attachment. A breach may also include the loss or theft of physical documents that include PU and portable electronic storage media that store PU, the inadvertent disclosure of PU on a public website, or an oral disclosure of PII to a person who is not authorized to receive that information. It may also include an authorized user accessing PU 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" .

X. HHSAR Provision, 352.239-73: Electronic and Information Technology Accessibility Notice

Contracts with entities that collect, maintain, use, or operate Federal information or information systems on behalf of CDC shall include the following requirements:

1) The contractor shall cooperate with and exchange information with CDC officials, as deemed necessary by the CDC Breach Response Team, to report and manage a suspected or confirmed breach.

2) All contractors and subcontractors shall properly encrypt PII in accordance with OMB Circular A-130 and other applicable policies, including CDC-specific policies, and comply with HHS-specific policies for protecting PII. To this end, all contractors and subcontractors shall protect 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.

3) All contractors and subcontractors shall participate in regular training on how to identify and report a breach.

4) All contractors and subcontractors shall report a suspected or confirmed breach in any medium as soon as possible and without unreasonable delay, consistent with applicable CDC IT acquisitions guidance, HHS/CDC and incident management policy, and United States Computer Emergency Readiness Team (US-CERT) notification guidelines. To this end, the Contractor (and/or any subcontractor) shall respond to all alerts/Indicators of Compromise (IOCs) provided by HHS Computer Security Incident Response Center (CSIRC) or CDC Computer Incident Response Team (CSIRT) within 24 hours via email at cdc@csirt.gov or telephone at 866-655-2245, whether the response is positive or negative.

5) All contractors and subcontractors shall be able to determine what Federal information was or could have been accessed and by whom, construct a timeline of user activity, determine methods and techniques used to access Federal information, and identify the initial attack vector.

6) All contractors and subcontractors shall allow for an inspection, investigation, forensic analysis, and any other action necessary to ensure compliance with HHS/CDC Policy and the HHS/CDC Breach Response Plan and to assist with responding to a breach.

7) Cloud service providers shall use guidance provided in the FedRAMP Incident Communications Procedures when deciding when to report directly to US-CERT first or notify CDC first.

8) Identify roles and responsibilities, in accordance with HHS/CDC Breach Response Policy and the HHS/CDC Breach Response Plan. To this end, the Contractor shall NOT notify affected individuals unless and until so instructed by the Contracting Officer or designated representative. If so instructed by the Contracting Officer or representative, all notifications must be pre-approved by the appropriate CDC officials, consistent with HHS/CDC Breach Response Plan, and the Contractor shall then send CDC- approved notifications to affected individuals; and,

9) Acknowledge that CDC will not interpret report of a breach, by itself, as conclusive evidence that the contractor or its subcontractor failed to provide adequate safeguards for PII.

D. 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).

E. 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 by the effective date of this contract. Any revisions to the roster as a result of staffing changes shall be submitted immediately upon 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.

F. Contract Initiation and Expiration

1) **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).

2) **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.

3) **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.*

4) **Notification.** The Contractor (and/or any subcontractor) shall notify the CO and/or

COR and system ISSO before an employee stops working under this contract.

5) **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 *CDC* policies.

6) The Contractor (and/or any subcontractor) shall perform and document the actions identified in the CDC Out-Processing Checklist (http://intranet.cdc.gov/od/hcrmo/pdfs/hr/Out_Processing_Checklist.pdf) when an employee terminates work under this contract. All documentation shall be made available to the CO and/or COR upon request.

G. 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 policies and shall not dispose of any records unless authorized by HHS.

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 policies.

Schedule of Deliverables

Deliverable Title/Description	Due Date
Roster	Before effective date of this contract
Contractor Employee Non-Disclosure Agreement (NDA)	Prior to performing any work on behalf of HHS
Assist in the completion of a PTA/PIA form	In conjunction with contract award
Copy of training records for all mandatory training	In conjunction with contract award and annually thereafter or upon request
Signed ROB for all employees	Initiation of contract and at least annually thereafter
Incident Report (as incidents or breaches occur)	As soon as possible and without reasonable delay and no later than 1 hour of discovery

Deliverable Title/Description	Due Date
Incident and Breach Response Plan	Upon request from government
List of Personnel with defined roles and responsibilities	Prior to performing any work on behalf of HHS
Off-boarding documentation, equipment and badge when leaving contract	At contract expiration after the Government's final acceptance of the work under this contract, or in the event of a termination of the contract.
Onboarding documentation when beginning contract.	Prior to performing any work on behalf of HHS
Form or deliverables required by CDC.	At contract expiration.
If the procurement involves a system or cloud service, additional documentation will be required, such as Disposition/Decommission Plan	At contract expiration.

HHSAR Provision, 352.239-73: Electronic and Information Technology Accessibility Notice

(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 when Federal agencies develop, procure, maintain, or use electronic and information technology, Federal employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who are not individuals with disabilities, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency.

(b) Accordingly, any offeror responding to this solicitation must comply with established HHS EIT accessibility standards. Information about Section 508 is available at http://www.hhs.gov/web/508. The complete text of the 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 contract are: 1194.

205 WCAG 2.0 Level A & AA Success Criteria
302 Functional Performance Criteria
502 Inoperability with Assistive Technology
504 Authoring Tools
602 Support Documentation
603 Support Services

In order to facilitate the Government's determination whether proposed EIT supplies meet applicable Section 508 accessibility standards, offerors must submit an HHS Section 508 Product Assessment Template, in accordance with its completion instructions. The purpose of the template is to assist HHS acquisition and program officials in determining whether proposed EIT supplies conform to applicable Section 508 accessibility standards. The template allows offerors or developers to self-evaluate their supplies and documentation detail - whether they conform to a specific Section 508 accessibility standard, and any underway remediation efforts addressing conformance issues. Instructions for preparing the HHS Section 508 Evaluation Template are available under Section 508 policy on the HHS Web site http://hhs.gov/web/508.

In order to facilitate the Government's determination whether proposed EIT services meet applicable Section 508 accessibility standards, offerors must provide enough information to assist the Government in determining that the EIT services conform to Section 508 accessibility standards, including any underway remediation efforts addressing conformance issues.

(d) Respondents to this solicitation must identify any exception to Section 508 requirements. If a offeror claims its supplies or services meet applicable Section 508 accessibility standards, and it is later determined by the Government, i.e., after award of a contract or order, that supplies or services delivered do not conform to the accessibility standards, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its expense.

(e) Electronic content must be accessible to HHS acceptance criteria. Checklist for various formats are available at http://508.hhs.gov/, or from the Section 508 Coordinator listed at https://www.hhs.gov/web/section-508/additional-resources/section-508-contacts/index.html. Materials that are final items for delivery should be accompanied by

the appropriate checklist, except upon approval of the Contracting Officer or Representative.

OFFICE OF THE ASSOCIATE DIRECTOR FOR COMMUNICATION
Request for Quote (RFQ) Form
For Ordering Off OADC Communication Services BPA

Part 3. Performance Work Statement

I. BACKGROUND AND NEED:

Smoking remains the leading cause of preventable death and disease in the United States, killing more than 480,000 Americans each year. Smoking takes a devastating toll on our nation's economy—costing more than $300 billion a year (nearly $170 billion in direct medical care for adults and more than $156 billion in lost productivity). According to the 2014 Report of the Surgeon General, *The Health Consequences of Smoking—50 Years of Progress,"* damage from tobacco smoke is immediate. Inhaling the multitude of chemicals and compounds in tobacco smoke—more than 7,000— causes immediate and long-term damage and leads to disease and death. Smoking longer means more damage. The only proven strategy for reducing the risk for tobacco-related disease and death is to never smoke, or to quit use of tobacco products.

Nine out of ten adult smokers start smoking before the age of 18. Each day in the U.S. about 1,600 youth under 18 years of age smoke their first cigarette and nearly 200 youth under 18 years of age become daily cigarette smokers. If cigarette smoking continues at the current rate among youth in this country, 5.6 million of today's Americans younger than 18 will die early from a smoking-related illness. That's about 1 of every 13 Americans aged 17 years or younger who are alive today.

The Centers for Disease Control and Prevention (CDC) is at the forefront of the nation's efforts to reduce deaths and prevent chronic diseases that result from tobacco use. CDC's Office on Smoking and Health (OSH) provides national leadership for a comprehensive, broad-based approach to reducing tobacco use. OSH's goals are to:

- Prevent initiation of tobacco use among youth and young adults
- Promote quitting among adults and youth
- Eliminate exposure to secondhand smoke
- Identify and eliminate tobacco-related disparities

Essential elements of this approach include state-based, community-based, and health system-based interventions; cessation services; counter-marketing; policy development and implementation; surveillance; and evaluation. These activities target groups that are at the highest risk for tobacco-related health problems. OSH accomplishes these goals by expanding the science base of tobacco control; building capacity to conduct tobacco control programs; communicating information to constituents and the public; and facilitating concerted action with and among partners.

A critical task includes coordinating publication dissemination as well as earned and news media activities. Key initiatives in the office include:

CDC's National Tobacco Education Campaign: CDC developed a national tobacco education campaign, *Tips From Former Smokers® (Tips®),* to educate adults who smoke about the harmful effects of smoking and tobacco use and encourage them to quit, and to encourage nonsmokers to protect themselves and their loved ones from secondhand smoke exposure. All ads include a call to action that directs people to a variety of free resources designed to help people who smoke to quit. These include a 1-800-QUIT-NOW telephone number which links callers to trained cessation coaches, a website URL at cdc.gov/tips that contains campaign information as well as links to a variety of free cessation resources, texting resources and links to applications.

The *Tips®* campaign is based upon scientific literature indicating that ads that graphically link smoking to health damage, evoke strong negative emotions, and that include personal testimonials are an effective way to promote cessation in adults and to prevent smoking initiation with young adults. First, in 2010, CDC ran a regional pilot campaign in the southeastern and southwestern U.S. with existing ads via radio, print, and outdoor media to promote smoking cessation. Next, in 2011, CDC developed its first paid media national campaign about smoking cessation with original, testimonial-style ads featuring actual former smokers who discussed health effects they suffered from cigarette smoking; this campaign that ran in 2012 reached its target audience via television, radio, print, outdoor ads, partnerships, and earned media. CDC ran the subsequent phases of the campaign from 2013 to 2019, with additional ads, spokespeople, and health conditions and will launch new ads in 2020.

Surgeon General's Reports: A critically important tobacco control tool for educating the public, updating and improving the science base, enhancing federal regulatory initiatives, and providing current data to policy leadership on the state, tribal, and national levels is the Surgeon General's Report (SGR). OSH is responsible for coordinating the development, clearance, and promotion of SGRs on tobacco use. OSH works closely with the Surgeon General's office and the Department of Health and Human Services to develop an aggressive marketing plan, including public relations activities and innovative, supporting materials to maximize the impact of the SGR.

In advance of each SGR release, OSH typically develops and tests a wide range of products to reach key audiences, including a 30-second public service announcement with supporting materials to further promote communication the messages in states and communities (i.e. pdfs for posters, infographics, etc.); a consumer guide in English and Spanish that uses visually exciting design and plain language to make the science in the SGR more accessible to the public; and press kits, sound bites, and b-roll to help reporters tell the SGR story. OSH is responsible for the creation of on-site event materials such as press kits, posters, signage and other items related to the promotional or release events, as well as online resources (website) and social media initiatives and opportunities. Finally, OSH conducts outreach to major media to expand coverage of the report's release, including coordination of background interviews and a satellite media/radio tour with the Surgeon General and key SGR contributors.

II. PROJECT OBJECTIVE:

The purpose of this contract is to provide support for earned media and news media activities conducted by OSH. These activities include, but are not limited to, technical assistance in communication and marketing; media planning; earned media strategy; media training and interview preparation; and technical writing and communications services. The contractor will also be expected to work with OSH to support activities associated with CDC's National Tobacco Education Campaign.

At the completion of this project, the following objectives shall be met:

1. To develop a comprehensive earned media and public relations plan for all three phases of each major release as defined by OSH: pre- release, release, and post-release, including measurable objectives and crisis communications; earned media strategies; recommended tactics for media outreach, promotion and dissemination; channels for distribution; media lists for national, local and trade media outreach; detailed timeline and work plan that identify roles and responsibilities.
2. To disseminate OSH initiatives using best practices for communication development, with an emphasis on reaching identified audiences;
3. To improve dissemination of OSH's products and information, including the use of media relations, to reach specific audiences.

III. DESCRIPTION OF WORK:

The contractor shall provide support for the dissemination of scientific findings and health communication materials through a variety of channels to a variety of audiences. Specifically, the contractor shall provide support for the public release of various scientific reports, articles, and health communication materials to launch national initiatives including, but not limited to, Surgeon General Reports (SGRs) on tobacco use and other high profile HHS/CDC reports, publications (such as Morbidity and Mortality Weekly Report (MMWR) articles, journal articles, and other major publications), campaigns (such as the national tobacco education campaign, currently known as *Tips From Former Smokers*® [Tips] campaign), and other projects, throughout the duration of the contract. Major media events described below would include, but are not limited to, SGR releases (e.g., press conference) and media campaign launches/activities (e.g. press conference, local market media tours).

In the base period, there will be no more than 9 activities, which could include:

- Two (2) *Tips From Former Smokers*® events;
- Seven (7) MMWR releases or peer reviewed journal articles.

In option years 1-4, there will be no more than 10 activities per performance period, which could include:

- One (1) Surgeon General's report launch;
- Two (2) *Tips From Former Smokers*® events;

- Seven (7) MMWR releases or peer reviewed journal articles.

Specific tasks include the following:

Task Order Management, Logistics, and Support:

1. The contractor shall provide an overall workplan that includes a plan for each task, staffing plan, and timeline within 30 business days of award. The contractor shall provide an update annually within 30 business days of the award of each new option year.

2. The contractor shall coordinate a kick-off meeting in Atlanta, GA with the COR and End User within 45 business days of award to review the technical requirements of contract, contractor's staffing plan, and a plan for each task.

3. The contractor shall provide a written summary of the kickoff meeting (Task #2) within 10 business days of the meeting.

4. The contractor shall participate in one additional in-person meeting in Atlanta to discuss project progress in the base year, and two in-person meetings in each subsequent option year.

5. The contractor shall provide a written summary of the meetings in Task #4 within 10 business days of the meeting.

6. The contractor shall provide work plans with timelines per activity as directed by the COR.

7. The contractor shall provide monthly progress reports showing work performed, progress on production, plans for next month, and any problems encountered or anticipated. This report should include a quality control element showing what problems, if any, have been identified and what measures have been or will be taken to overcome them.

8. The contractor shall provide a year-end report at the conclusion of each performance period summarizing all activities.

9. The contractor shall provide shipments of materials as directed by the COR.

10. The contractor shall inventory all media assets of each project upon completion of each activity and provide these materials to OSH. All work conducted under this task order is considered property of HHS/CDC/OSH, including but not limited to media planning documents, final media materials or reports, print materials, and infographics.

Earned Media and News Media Activities

11. The contractor shall provide a comprehensive, written plan for each major media event. The plan shall include projected general audience media outreach and earned media activities. The plan shall also include an overview section, goals and measurable objectives (including sample measures for earned media), recommended earned media strategies and tactics to ensure successful media coverage, media campaign dissemination recommendations, channels, a timeline, media distribution/targeted media lists, and roles and responsibilities.

12. The contractor shall provide technical assistance, public relations logistical support (such as identifying availability of campaign(s) participants for media opportunities), coordinate and facilitate campaign(s) participant travel and participation in media activities, and make recommendations for media outreach and earned media activities. The cost of campaign participants' travel is not a deliverable in this contract.

13. The contractor shall develop an outreach plan for specific audience segments using the criteria established in the general audience media outreach plan (referenced in the Task #11). In addition to standard media channels, the contractor shall support access to minority media and minority organizations in media plans, as directed by CDC. The contractor shall provide access to specific audience media outlets (digital and traditional) and involve specific audience organizations in marketing plans. Reaching specific audiences through digital media channels and strategies (e.g. bloggers) should be strongly considered.

14. The contractor shall handle all the logistical arrangements associated with major media events (i.e. SGR or Tips) (including making recommendations for and securing the venue, producing press kits, developing and disseminating invitations, managing electronic/online RSVPs, arranging for on-site VIPs, securing all necessary AV equipment, staffing the media registration table, producing signage, and other items related to the event or activity).

15. The contractor shall secure donated/earned media and pitch stories each month throughout the performance period, including up to one major pitch per month per performance period.

16. The contractor shall organize meetings with editorial boards at various media publications.

17. The contractor shall develop b-roll and provide access to other media-related materials (including but not limited to stock video and photos).

18. The contractor shall write media-related remarks or speeches, including coordination of photo and graphic elements (e.g. PowerPoint slides), as requested by CDC.

19. The contractor shall provide photography services for major media events, such as SGR or campaign releases, as requested by CDC.

20. The contractor shall identify and recommend long-lead media strategies that will support key messages.

21. The contractor shall provide daily media monitoring as well as analyses of the media coverage following each major media event. Coordination of no more than 3 major launch events per performance period are anticipated (e.g., SGR, campaign launch). *(Note: upon award, contractor will have access to previous examples of daily and post-launch media coverage reports).*

22. The contractor shall develop press materials including press releases, fact sheets, and speaker bios.

23. The contractor shall assemble and provide press packets to CDC that contain materials developed in Item #22, as directed by CDC.

24. The contractor shall develop message maps and talking points/scripted remarks for use by CDC and HHS spokespeople when they are participating in media relations activities, including but not limited to press events.

25. Prior to any major media events and in coordination with an ongoing need to grow the number of OSH staff capable of speaking to the news media, the contractor shall facilitate media training for CDC, HHS, and/or campaign(s) spokespersons that will take part in interviews or participate in media events. This media training shall include a refresher of message delivery and media interview guidelines. The training shall also include mock interview scenarios for each potential spokesperson to enable them to practice using the messaging and sitting for a media interview. The contactor shall provide a camera for these interviews to allow for playback of the mock scenarios and a very basic critique. During those sessions, the contractor shall work with the spokespeople to develop and customize messaging. For budget purposes, the contractor shall plan on up to six media training sessions per performance period.

26. The contractor shall establish a protocol for assisting CDC with inquiries received from members of the news media, drafting responses, and potentially responding to these inquiries.

27. The contractor shall provide recommendations regarding risk and crisis communication and associated messages/talking points.

28. For CDC's National Tobacco Education Campaign (e.g., *Tips From Former Smokers*®), the contractor shall be poised to implement an ad participant post-mortem plan. The contractor shall plan on one per performance period. This plan shall reflect specific steps that CDC and the contractor shall undertake should an ad participant pass away.

29. The contractor shall provide coordination, promotion, and production of editorial board, radio, satellite, social media, or local market media tours as directed by CDC. CDC must approve all spokespeople. Each satellite and radio media tour shall target national, regional, and/or local media, as determined by CDC. If radio tours or satellite media tours are selected as part of the promotion strategy, interviews shall be done with stations, both in English and Spanish. If social or digital media promotions are considered, the contractor shall determine live chat or other appropriate interactive formats to promote the campaign(s). If local market media tours are selected as part of the promotion strategy, the contractor shall provide assistance to CDC, state health departments, local health departments, and/or other tobacco control partners involved. Activities may include but are not limited to media interviews with print reporters and/or at radio and television stations; press conferences with state or local health departments, campaign ad participants, and/or partners/stakeholders; media roundtable discussions with campaign ad participants as well as state and/or community representatives; panel discussions between campaign ad participants and community leaders or local stakeholders; and meet and greets with campaign ad participants. (Note: upon award,

contractor will have access to previous examples of local market media tours). The contractor shall provide a proposal of key messages to be used during the promotional tours and a schedule of the dates and times two weeks prior to the tour. The contractor shall plan on up to three promotional tours per performance period.

30. The contractor shall translate OSH's scientific and communication products for general audiences and media. These materials include, but are not limited to, presentations, fact sheets, questions and answers, key messages, media infographics, talking points or scripted remarks, press releases, media advisories, media statements, biographies, press kit folders, and other media materials to be included in press kits.

    While the Surgeon General Report releases require the most extensive communication product development and support, it is anticipated that the contractor will assist in communication product development for up to two major release/products in the base period, and up to 3 during performance periods 1-4.

    Materials shall be written following plain language principles and practices.

    HHS policy requires that health-related media products receive approval from the Office of the Assistant Secretary for Public Affairs (ASPA) before release to the public. The contractor shall submit the necessary clearance packages, which shall include required forms and supporting materials (e.g., draft text or storyboards). Required forms must be completed in accordance with the HHS Public Affairs Management Manual—*www.hhs.gov/hhsmanuals/public_affairs.pdf*. Materials shall be approved before final copy or production can be initiated.

    All materials must satisfy all 508 requirements. For graphics (print and web) materials, this means ensuring that all content passes all 508 testing. For video products, closed-captioning files will be prepared and delivered to the customer for viewers who are hearing-impaired, and audio description files (in WAV and MP3 formats) for viewers who are vision-impaired) will have to be prepared.

31. The contractor shall provide graphic design services needed for media-related communications, e.g., the development of infographics, illustrations, drawings, photographs, slides, and other similar visual materials. The contractor shall follow all required HHS and CDC clearance procedures as well as the requirements and guidelines for printing. The contractor shall use the latest version of Adobe Creative Suite to produce all campaign materials and products. Print materials will be created in accordance with Government Printing Office (GPO) rules and regulations (http://www.gpoaccess.gov/stylemanual/index.html; http://www.gpo.gov/pdfs/customers/sfas/jcpregs.pdf). All materials prepared for television, print, or radio must be in a format that is appropriate for Internet and new media use, including being 508 compliant. All PowerPoint presentations shall adhere to CDC guidelines (e.g., use approved template, fonts, logos, etc.).

32. The contractor shall pay any publication fees associated with manuscripts, news articles, etc.

(anticipate payment of 2 fees per year). **Important material development guidelines:** Emphasis shall be on economy and quality, with attention to the current restrictions on government printing and audiovisual production.

33. The contractor shall provide written releases for all talent and directors used in the production of materials. When at all possible, all releases for talent, images, graphics, music, and other elements shall be obtained on a 100%-buyout basis, and the contractor should appropriately select elements to achieve the buyout at low cost. The contractor shall provide a summary table for each printed product it produces that shows each image purchased, indicates the pages on which the images appear, identifies the photo collection from which each image was purchased, and summarize the usage rights for each image. All materials will be produced in the media formats, lengths, and technical specifications according to broadcast-quality standards.

IV. DELIVERABLES:

All task order deliverables intended for communication to the public must comply with Public Law 111–274, the Plain Writing Act of 2010. For Plain Language information and the Federal Plain Language Guidelines see www.plainlanguage.gov.

TASK ORDER MANAGEMENT, LOGISTICS, AND SUPPORT						
		Quantity				
Task	**Item**	**Base Period**	**Option Years 1-4**	**Delivery Method**	**Deliver To**	**Due Date**
1	Overall task order work plan, timeline	1	1 each year	Report in Word submitted via email	COR and End User	Within 30 business days of award
2	Kick-off meeting in Atlanta	1	None	In person	COR and End User	Within 45 business days of award
3	Kick-off meeting summary	1	None	Report in Word submitted via email	COR and End User	Within 10 business days of the meeting
4	Travel to Meetings in Atlanta	2 [two travelers] *[includes kickoff meeting]*	NTE 3 each year [two travelers]	In person	COR and End User	As directed by the COR and coordinated with OSH
5	Meeting summary	1	NTE 3 each year	Report in Word submitted via email	COR and End User	Within 10 business days of the meeting
6	Work plans/timelines per activity	I per activity/NTE 9	NTE 10 each year	Report in Word submitted via email	COR and End User	Within 14 business days of assigned project
7	Monthly progress reports	6	12 each year	Report in Word submitted via email	COR and Contracting Officer	Monthly; by the 10th business day of each month
8	Year-end summary report	1	1 each year	Report in Word submitted via email	COR and End User	Report must be delivered on or before the end of each performance
9	Packages and shipments	NTE 10	NTE 10 per year	Mail or expedited shipping	COR and End User	Ongoing throughout each performance period as directed

10	Project data and property transfer	1 per activity/NTE 9	NTE 10 per year	Electronically through email and/or mail, expedited shipping	COR and End User	Within 14 business days of end of project

EARNED MEDIA AND NEWS MEDIA ACTIVITIES						
Task	**Item**	**Quantity**		**Delivery Method**	**Deliver To**	**Due Date**
		Base Period	**Option Year 1-4**			
11	Media outreach and earned media plan	2	NTE 3 per year	Report in Word submitted via email	COR and End User	Within 14 business days of assigned
12	Technical Assistance/ Logistical support	1 per activity/NTE 9	1 per activity/NTE 10 per year	Confirmation via email	COR and End User	Ongoing as directed by the COR
13	Media outreach plan for specific audience segments	1 plan per activity/ NTE 9	1 plan per activity/NTE 10 per year	Report in Word submitted via email	COR and End User	Yearly beginning 3 months prior to campaign(s)
14	Logistics for press events	NTE 2	NTE 2 per year	Confirmation via email	COR and End User	Planning will begin no later than 3 months prior to campaign(s) and/or publication
15	Pitch stories for donated/earned media	NTE 6	NTE 12 per year	Confirmation via email	COR and End User	Monthly as directed by the COR
16	Organize meetings with editorial boards	NTE 1	NTE 1 per year	Confirmation via email	COR and End User	Ongoing as directed by the COR
17	Develop b-roll and other media related materials	NTE 3	NTE 7 per year	Drafts via email	COR and End User	Ongoing as directed by the COR
18	Write speeches	NTE 3	NTE 6 per year	Drafts in Word submitted via email	COR and End User	Ongoing as directed by the COR
19	Photography Services	NTE 6	NTE 12 per year	Drafts submitted via email	COR and End User	Ongoing as directed by the COR
20	Develop long-lead media strategies	NTE 2	NTE 4 per year	Report in Word submitted via email	COR and End User	Within 14 business days of assigned project

21	Daily media monitoring and post-event media analysis report	NTE 2	NTE 3 per year	Report submitted via email	COR and End User	14 business days after the event
22	Develop press releases, fact sheets, speaker bios, message maps, talking points/scripted remarks	NTE 2 of each product	NTE 3 of each product per year	Drafts in Word submitted via email	COR and End User	Ongoing as directed by the COR
23	Press kits	NTE 50	NTE 250 per year	Via mail/expedited shipping	COR and End User	At least one business day before event
24	Develop message maps, talking points, scripted remarks	NTE 2	NTE 3 of each product per year	Drafts in Word submitted via email	COR and End User	Ongoing as directed by the COR
25	Conduct media training sessions	NTE 2	NTE 6 per year	In person	COR and End User	Ongoing as directed by the COR
26	Establish protocol for responding to media inquiries	1	1 each year (if revisions are necessary)	Draft is Word via email	COR and End User	Within first 30 business days of the
26	Draft responses/Respond to media inquires	NTE 5	NTE 10 per year	Draft is Word via email	COR and End User	Ongoing (Within 1-4 hours pending media
27	Provide recommendations regarding risk/crisis communications	NTE 5	NTE 10 per year	Report in Word via email	COR and End User	Ongoing as directed by the COR
28	Campaign Ad Participant Post-Mortem Plan	1	1 per year	Report in Word via email	COR and End User	Within first 30 buiness days of the contract award
29	Media Tours	NTE 2	NTE 3 per year	Confirmation electronically through email	COR and End User	Ongoing as directed by the COR
30	Develop plain language materials for major OSH reports and other initiatives	NTE 2 sets	NTE 3 sets per year	Drafts in Word via email	COR and End User	Ongoing as directed by the COR
31	Provide graphics services for all materials developed	NTE 6	NTE 12 per year	Adobe via email	COR and End User	Ongoing as directed by the COR

32	Pay publication fees	NTE 2	NTE 2 per year	Confirmation electronically through email	COR and End User	Ongoing as directed by the COR
33	Provide summary of written releases for all talent used in materials	Ongoing, as needed	Ongoing, as needed	Report in Word via email	COR and End User	Ongoing as directed by the COR

All materials must be submitted electronically in MS compatible format that meets CDC standards and is readily available at CDC (e.g. MS Office (Word, Excel, PowerPoint) or Adobe Acrobat. All reporting requirements and written deliverables as part of this contract will be supplied to the project Contracting Officer Representative (COR). Acceptance of any written deliverables is pending CDC COR review and correction to any resulting comments, to be confirmed in writing and documented in the closest following monthly report. Any schedule of interim deliverables may be revised according to CDC acceptance of an updated written work plan by the COR during the project with the restriction that these changes must not impact the overall period of performance, scope, or specifications of the award, or otherwise impinge on the authority of the contracting officer. It is the responsibility of the contractor to fully understand what changes require contracting officer approval.

V. PERFORMANCE MATRIX:

Work Requirement	Acceptable Quality Level (AQL)	Monitoring Method	Incentives/ Disincentives
Task 2 *Kick off meeting*	• Occurs at the beginning of the project • Contractor is prepared to discuss relevant project issues, is responsive to project planning issues/project improvements, and documents meetings as described in PWS (may be corrected to COR comments)	• 100% review of event (by the COR) • Unacceptable meetings will be documented as customer complaints, contractor may be allowed to correct any insufficiences to CDC satisfaction	• Contractor's performance is documented as past performance using CPARS which is considered for future awards.
Tasks 1, 3-33 *Meet all production deadlines as directed by the COR*	• Contractor consistently meets timelines, as described in the PWS and directed by the COR. Any issues are brought to the attention to the COR as soon as they are identified and solutions are presented.	• 100% review of event (by the COR) • Unacceptable performance will be documented as customer complaints, contractor may be allowed to correct any insufficiences to CDC satisfaction	• Repeated complaints on different events/tasks but the same issue will be elevated for higher level resolution (senior management and/or Contracting

Work Requirement	Acceptable Quality Level (AQL)	Monitoring Method	Incentives/ Disincentives
			Officer)

VI. PERIOD OF PERFORMANCE:

The contract period of performance will consist of one (1) 6-month base period and four (4) 12-month optional periods for a maximum potential period of performance of 54 months, if all option periods are exercised. The deliverables and quantities for option periods are noted in the deliverables chart below.

Base Year	9/30/2020-3/31/2021
Option Year 1	4/1/2021-3/31/2022
Option Year 2	4/1/2022-3/31/2023
Option Year 3	4/1/2023-3/31/2024
Option Year 4	4/1/2024-3/31/2025

VII. PLACE OF PERFORMANCE:

Work for this task order shall be performed off-site. The Contractor will not be required to be located, or to maintain a local office in the Atlanta, Georgia, area. However, if the Contractor is located in a distant geographical location, they will be required to schedule regular conference call and travel to Atlanta for face-to-face meetings with the COR and End User as specified in the PWS to facilitate close working relationships with CDC's project staff.

All travel shall be in accordance with the Federal Travel Regulations (FTR) and the Joint Travel Regulations (JTR) and adhere to FAR 31.205-46. The contractor shall ensure that the requested travel costs will not exceed the amount authorized in this task order. Travel must be submitted to COR in an official request with anticipated expenses and justification.

Prior Approval: Requests for travel approval shall:

- Be prepared in a legible manner
- Include a description of the purpose of the trip
- Be summarized by traveler
- Identify the task order number
- Identify the task order CLIN
- Be submitted in advance of the travel with sufficient time to permit review and approval

All travel must be authorized by the COR and be in compliance with the task order and all other applicable requirements.

The contractor shall use only the minimum number of travelers and rental cars needed to accomplish the trip purpose. Travel shall be scheduled during normal duty hours whenever possible. Airfare will be reimbursed for actual common carrier fares which are obtained by the most reasonable and economical means.

The contractor shall provide a Trip Report for each trip associated with a travel approval. The contractor shall maintain a summary of all approved travel, to include at a minimum, the name of the traveler, location of travel, duration of trip, total cost of trip.

Kick-off/orientation meeting: The contractor will participate in a kick-off meeting with CDC to review the strategy, goals, objectives, and associated tasks related to this PWS. This meeting will serve as the time for all parties to establish working relationships, discuss expectations and CDC requirements, as outlined in the PWS, as well as initial steps to develop the most effective strategies. The contractor may also be required to attend a kickoff meeting for the national tobacco education campaign. In an effort to maximize travel dollars, the latter meeting should occur prior to or immediately following the former. The contractor will plan for 2 to 3 full working days for these kick-off meetings.

In-Person planning meetings: The contractor will budget for up to two in-person meetings each year with key contract staff. The in-person meetings will consist of one large meeting with OSH leadership and smaller workgroup meetings with key OSH staff. In an effort to maximize travel dollars, the latter meeting should occur prior to or immediately following the former. During these meetings, the contractor will come prepared to recommend media strategy, share new and innovative practices from the field, and share relevant information with attendees. The contractor will be responsible for preparing presentation materials and capturing notes on key topic areas and action items.

Note: As many of the activities, sub-activities and activities in this larger task order involve training and technical assistance, minimal travel by a couple of key staff members may be necessary at points during the task order period. If appropriate, the Task Order COR will approve of plans and adjust other deliverables accordingly.

VII. GOVERNMENT FURNISHED MATERIALS, FACILITIES AND PROPERTY

1. **Supplying the contractor with GFP/GFE/GFF/GFI.**
   CDC/OSH will provide facilities, equipment, and supplies when contract staff is required to work at CDC/OSH sites. CDC will provide any new scientific or health communication materials from our office that are relevant to these activities during the duration of the project.

2. **Accounting for GFP/GFE/GFF/GFI.** As discussed in the PWS, the contractor will be responsible for a data and property transfer before project is complete.

SECURITY OF GOVERNMENT FACILITIES, INFORMATION, AND INFORMATION SYSTEMS.

(i) **HSPD-12.**
HSPD-12 is not applicable, as the Contractor will not have routine physical access to federally controlled facilities and/or routine access to federally controlled information systems.

(ii) **Privacy Act.**
The consumer research information that the contractor will obtain as part of materials development and testing are subject to the Privacy Act. The contractor will comply with standard commercial protections to ensure the safeguarding of these data.

(iii) **Federal Information Security Management Act (FISMA).**
FISMA is not applicable to the proposed acquisition, as the Contractor will not obtain sensitive information or develop information systems posing potential security risks.

(iv) **Contractor Access to Sensitive Information.**
The Contractor will not obtain sensitive information or develop information systems posing potential security risks

Requirements for Information Security and/or Physical Access Security

VIII. Information Security Requirements

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. Protect 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:	[X] Low [ ] Moderate [ ] High
Availability:	[X] Low [ ] 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:

[ ] No PII [X] 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 "*handling*" 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 protect its confidentiality, integrity, and/or availability. The Contractor (and/or any subcontractor) shall protect 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 and CDC policies. Unauthorized disclosure of information will be subject to the HHS/CDC 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 protect 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 and CDC-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 and ISSO within 30 days of contract award.
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 CDC non-disclosure agreement. 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 CDC 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 CDC SOP or designee with completing a PIA for the system or information within *30 days* 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 CDC 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.

A. 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/CDC 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 *CDC specific* 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.

B. 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*, and any CDC-specific rules, as applicable.
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 CDC 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.

C. 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)/CDC CSIRT 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) Protect all sensitive information, including any PII created, stored, or transmitted in the performance of this contract 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 CDC approved notifications to affected individuals following CDC's designated process.
3) Report all suspected and confirmed information security and privacy incidents and breaches to the CDC's Computer Security Incident Response Team (CSIRT) *[CSIRT@CDC.gov]*, COR, CO, CDC 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 CDC and 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 and CDC's 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.

D. 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 position sensitivity designation levels that apply to this solicitation/contract will be determined after award. The levels will be 1) Not applicable, 2) Level 1: Non-sensitive, and/or 3) Level 5: Public Trust/Moderate Risk.

E. 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. For additional information, see HSPD-12 policy at:* https://www.dhs.gov/homeland-security-presidential-directive-12)

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, can access, or host and/or maintain a government information system(s). The roster shall be submitted to the COR and/or CO within the CDC Specified

timeline of the effective date of this contract. Any revisions to the roster as a result of staffing changes shall be submitted within 7 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.

F. Contract Initiation and Expiration

1) **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 CDC EPLC framework and methodology and in accordance with the HHS Contract Closeout Guide (2012). CDC EPLC requirements may be located here: https://www2a.CDC.gov/CDCup/library/other/eplc.htm.
2) **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.
3) **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*.
4) **Notification.** The Contractor (and/or any subcontractor) shall notify the CO and/or COR and system ISSO within 7 days before an employee stops working under this contract.
5) **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 CDC policies.
6) The Contractor (and/or any subcontractor) shall perform and document the actions identified in the CDC Contractor Employee Separation Checklist when an employee terminates work under this contract within 7 days of the employee's exit from the contract. All documentation shall be made available to the CO and/or COR upon request.

G. 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/CDC policies and shall not dispose of any records unless authorized by HHS/CDC.

- If 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/CDC policies.

Requirements for Procurements Involving Privacy Act Records

A. Privacy Act

It has been determined that this contract is subject to the Privacy Act of 1974, because this contract provides for 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 SORN 09-20-0160, Records of Subjects in Health Promotion and Education Studies. HHS/CDC/CoCHP.

The design, development, or operation work the Contractor is to perform is outlined in the Statement of Work.

The disposition to be made of the Privacy Act records upon completion of contract performance will follow the CDC's Scientific and Research Project Records Control Schedule. The Contractor and any subcontractor must follow CDC records disposition instructions and as applicable, the corresponding Records Schedule.

Requirements for Government Information Processed on Government or Contractor Owner Systems

A. Security Requirements for Government Information Processed on Government or Contractor Owner Systems

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 protect 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 tbe ATO within the specified timeline(s). The Contractor shall conduct the SA&A requirements in accordance with *HHS IS2P, CDC's*

SA&A Standard Operating Procedures, NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (latest revision).

CDC's 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 a SA&A package to the C/I/O Information Systems Security Officer. 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 and CDC policies and other guidance. The SSP shall be consistent with and detail the approach to IT security contained in the Contractor's bid or proposal that resulted in the award of this contract. The SSP shall provide an overview of the system environment and security requirements to protect 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 a CDC assessor and be consistent with NIST SP 800-53A, NIST SP 800-30, and HHS and CDC policies. The assessor will document the assessment results in the SAR. Thereafter, the Contractor, in coordination with CDC shall assist in the assessment of the security controls and update the SAR at least ***annually***.
- **Independent Assessment** - When applicable, 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 CDC policies. All high-risk and medium weaknesses must be mitigated within CDC defined timeframes from the date the weaknesses are formally identified and documented. CDC 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, ***CDC*** may require designated POAM weaknesses to be remediated before an ATO is issued. Thereafter, the POA&M shall be updated at least ***quarterly*** or as requested by CDC.

- **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 and CDC 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 by specified due date provided by *CDC*.
- **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 annually. 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 annually, if not more often. The contractor shall maintain a capability to provide security configuration compliance information for 100% of its IT assets using SCAP-compliant automated tools.
- **Vulnerability Management** - 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 monthly.
- **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 CDC specified timeframes. CDC specific timeframes can be provided after contract award.
- **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 enough 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.

Requirements for Utilizing Cloud Services

A. HHS FedRAMP Privacy and Security Requirements

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

1) **FedRAMP Compliant ATO**. Comply with FedRAMP Security Assessment and Authorization (SA&A) requirements and ensure the information system/service under this contract has a valid FedRAMP compliant (approved) authority to operate (ATO) in accordance with Federal Information Processing Standard (FIPS) Publication 199 defined security categorization. If a FedRAMP compliant ATO has not been granted, the Contractor shall submit a plan to obtain a FedRAMP compliant ATO.

a. Implement applicable FedRAMP baseline controls commensurate with the agency-defined security categorization and the applicable FedRAMP security control baseline (www.FedRAMP.gov). The *HHS Information Security and Privacy Policy (IS2P)* and *HHS Cloud Computing and Federal Risk and Authorization Management Program (FedRAMP) Guidance* further define the baseline policies as well as roles and responsibilities. The Contractor shall also implement a set of additional controls identified by the agency when applicable.
b. A security control assessment must be conducted by a FedRAMP third-party assessment organization (3PAO) for the initial ATO and ***annually*** thereafter or whenever there is a significant change to the system's security posture in accordance

with the FedRAMP Continuous Monitoring Plan.

2) **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.
3) **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 *CDC* to develop and maintain an SLA.
4) **Interconnection Agreements/Memorandum of Agreements.** When applicable, the Contractor shall establish and maintain Interconnection Agreements and or Memorandum of Agreements/Understanding in accordance with HHS/CDC policies.

B. 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 protect it to the same extent they would the proprietary data and/or company trade secrets and in accordance with HHS/CDC 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 FedRAMP requirements and HHS 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/*CDC*. 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.

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

1) The Contractor (and/or any subcontractor) shall comply with HHS and FedRAMP 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/*CDC* security policies.

    a. In addition to the FedRAMP compliant ATO, 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 *CDC* authorizing official (AO) prior to implementation of system and/or service being acquired.
    b. CSP systems categorized as Federal Information Processing Standards (FIPS) 199 high must leverage a FedRAMP accredited third-party assessment organization (3PAO); moderate impact CSP systems must make a best effort to use a FedRAMP accredited 3PAO. CSP systems categorized as FIPS 199 low impact may leverage a non-accredited, independent assessor.
    c. For all acquired cloud services, the SA&A package must contain the appropriate documentation as determined. *The Contractor can refer to the deliverables mentioned in the FedRAMP Standard Contract Language available on the FedRAMP site.* Following the initial ATO, the Contractor must review and maintain the ATO in accordance with HHS/*CDC* policies.

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 FedRAMP 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 and high vulnerabilities no later than ***thirty (30) days*** and (2) medium and low vulnerabilities no later ***than sixty (60) days.*** In the event 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

FedRAMP baselines.

5) **Revocation of a Cloud Service**. HHS/*CDC* have 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 and FedRAMP security and privacy requirements and/or there is an incident involving sensitive information, HHS and/or *CDC* 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.

D. Reporting and Continuous Monitoring

1) Following the initial ATOs, the Contractor (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 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 CDC 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/CDC'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.

E. Configuration Baseline

1) The contractor 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/CDC configuration baseline.
2) The 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.

F. Incident Reporting

1) The Contractor (and/or any subcontractor) shall provide an Incident and Breach Response Plan (IRP) in accordance with HHS, CDC, OMB, and US-CERT requirements and obtain approval from the CDC. In addition, the Contractor must follow the incident response and US-CERT reporting guidance contained in the FedRAMP Incident Communications.
2) 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/*CDC* personnel, or agents acting on behalf of HHS/*CDC*, 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.

G. 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) *including appropriate actions such as logging and a documented chain of custody form.*
2) All information, devices and media must be encrypted with HHS-approved encryption mechanisms to protect the confidentiality, integrity, and availability of all government information transported outside of controlled facilities.

H. 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.

IX. HHSAR Provision, 352.239-73: Electronic and Information Technology Accessibility Notice

(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 when Federal agencies develop, procure, maintain, or use electronic and information technology, Federal employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who are not individuals with disabilities, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency.

(b) Accordingly, any offeror responding to this solicitation must comply with established HHS EIT accessibility standards. Information about Section 508 is available at http://www.hhs.gov/web/508. The complete text of the 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 contract are: 1194.

205 WCAG 2.0 Level A & AA Success Criteria
302 Functional Performance Criteria
502 Inoperability with Assistive Technology
504 Authoring Tools
602 Support Documentation
603 Support Services

In order to facilitate the Government's determination whether proposed EIT supplies meet applicable Section 508 accessibility standards, offerors must submit an HHS Section 508 Product Assessment Template, in accordance with its completion instructions. The purpose of the template is to assist HHS acquisition and program officials in determining whether proposed EIT supplies conform to applicable Section 508 accessibility standards. The template allows offerors or developers to self-evaluate their supplies and documentation detail - whether they conform to a specific Section 508 accessibility standard, and any underway remediation efforts addressing conformance issues. Instructions for preparing the HHS Section 508 Evaluation Template are available under Section 508 policy on the HHS Web site http://hhs.gov/web/508.

In order to facilitate the Government's determination whether proposed EIT services meet applicable Section 508 accessibility standards, offerors must provide enough information to assist the Government in determining that the EIT services conform to Section 508 accessibility standards, including any underway

remediation efforts addressing conformance issues.

(d) Respondents to this solicitation must identify any exception to Section 508 requirements. If a offeror claims its supplies or services meet applicable Section 508 accessibility standards, and it is later determined by the Government, i.e., after award of a contract or order, that supplies or services delivered do not conform to the accessibility standards, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its expense.

(e) Electronic content must be accessible to HHS acceptance criteria. Checklist for various formats are available at http://508.hhs.gov/, or from the Section 508 Coordinator listed at https://www.hhs.gov/web/section-508/additional-resources/section-508-contacts/index.html. Materials that are final items for delivery should be accompanied by the appropriate checklist, except upon approval of the Contracting Officer or Representative.

(End of provision)

Statement of Work
National Center for Injury Prevention and Control (NCIPC)
Division of Violence Prevention
Office of Policy, Partnerships and Strategic Communication
Contract for Media Evaluation and Monitoring

C.1 Background and Need

For more than 20 years, CDC's National Center for Injury Prevention and Control (the Injury Center) has helped protect Americans from injuries and violence. We are the nation's leading authority on injury and violence. We study violence and injuries and research the best ways to prevent them, applying science and creating real-world solutions to keep people safe, healthy, and productive. In the United States, injury is the leading cause of death for children and adults between the ages of 1 and 45. Injuries and violence affect everyone—regardless of age, race, or economic status. More than 3 million people are hospitalized, 27 million people are treated in emergency departments and released, and over 192,000 die as a result of violence and unintentional injuries each year.

The Division of Violence Prevention (DVP) is one of three divisions within NCIPC. Its mission is to prevent violence and its consequences so that all people, families, and communities are safe, healthy, and free from violence. DVP is committed to stopping violence before it begins (i.e., primary prevention). The division works to:

- Monitor violence-related behaviors, injuries, and deaths
- Conduct research on the factors that put people at risk for or protect them from violence
- Create and evaluate the effectiveness of violence prevention programs, practices, and policies
- Help state and local partners plan, implement, and evaluate violence prevention efforts
- Promote the effective adoption and dissemination of violence prevention strategies

C.2 Project Objective

The purpose of this project is to provide support for news media activities conducted by the DVP Office of Policy, Partnerships and Strategic Communication (OPPSC). These activities include, but are not limited to, evaluation of media coverage and messages, media monitoring, and message and audience analysis.

OPPSC evaluates news media coverage of violence prevention messages and how the topics are framed. For this project, the analysis of media will identify which issues are important to be aware of and explore the parameters of the discussion itself. This project will also focus on framing and measures including tone, prominence, and dominance. This will allow OPPSC to better understand the influence of media reporting on violence prevention and the potential benefits of message framing and monitoring for developing messages and products for journalists.

At the completion of this project, the following objectives shall be met:

- Determine if DVP media outreach strategies result in an increase in coverage
- Learn actionable insights that will help us understand that "why" behind our mentions and coverage
- Identify emerging issues that media are focused on
- Gain insight into the framing patterns and coverage accuracy related to DVP messages.

DVP will use the acquired information and data from this project to inform future media outreach strategies. DVP will build upon this work and measure the impact and perception of messages and evaluate the effectiveness of communications plans and campaigns.

C.3 Scope of Work

The contractor will be responsible for managing all aspects of DVP OPPSC's media evaluation and monitoring project. Specific activities may include:

Media Monitoring

Media monitoring services to track the growing number of priority topic mentions across all media; to track the reach of articles and data releases; have an archive of media mentions; and, to provide a daily media report, newsletter and archive of all media mentions. Tasks include but are not limited to:

- Television Monitoring – Monitoring of all 210 local U.S. DMA. Broadcast monitoring includes local market newscasts, nationally televised, syndicated content and cable news and cable programming.

- Radio Monitoring – Monitoring of the top 350+ terrestrial radio stations in the U.S.
- Internet News – Monitoring of 50,000+ news websites including the online editions of newspapers, magazines, trade publications, journals as well as television and radio station websites.
- Print Monitoring – Monitoring of print sources including top U.S. daily newspapers, magazines and trade publications.
- Web-Resolution News Clips – Self-edit and download unlimited web resolution news clips. Set video start and stop points and create downloadable files.
- Media Coverage – Monitoring of DVP- related media mentions. Results should be vetted and reviewed for accuracy by a human editor.
- Media Archive – Archive media coverage and have the ability to view, share or download your clips any time.
- Daily News Alerts – Receive daily email alerts detailing air date, time, station, newscast text summaries, preview video & audio, Nielsen audience numbers and publicity values for broadcast content.
- Unlimited Keywords – Includes set up of ongoing searches. Keywords can be modified any time to meet Client's needs
- Monitoring Portal - Anytime access to the dashboard housing your Media Coverage, Media Archive as outlined below.
- Daily Custom Newsletter—A filtered and branded email updated with key media hits for each topic monitored. Delivered via email by 1pm Eastern each day the report is due. Newsletter template to be reviewed and approved by CDC prior to implementation.

Media Analysis and Evaluation

- Analysis and evaluation of all DVP-related media mentions across traditional print, online, social and broadcast media. This project will also focus on framing and insights including tone, prominence, and dominance.
- Analysis and evaluation of media coverage for targeted media outreach efforts. Coordination of no more than 3 major media outreach efforts per performance period are anticipated (e.g., Vital Signs, special publications).
- An analysis and evaluation report for each effort is due 30 days after the effort. . Key performance indicators and measure included in report to be reviewed and approved by CDC prior to implementation.

C.4 Technical Requirements

The Contractor, as in independent organization and not an agent of the Government, shall furnish all labor, travel, and other costs, as required.

The contractor shall have:

- Knowledge of media monitoring, analysis, and evaluation practices
- Ability to communicate orally and in writing
- Strong organizational skills, attention to detail, and adherence to deadlines
- Ability to work in a fast-paced environment
- Experience working with senior leaders in an organization

C.5 **Reporting Schedule**

The Contractor shall provide, by the 5th business day of each month, a written report summarizing the status of contract activities. The report shall include a summary of completed tasks from the previous report and any outstanding items. The report shall be submitted to the Contracting Officer's Representative (COR).

C.6 **Training/Travel**

No cost training is anticipated for this position. If travel funds are required, the Government reserves the right to modify the contract to add funds. The contractor shall obtain approval from the Contracting Officers Representative (COR) and Contracting Officer (CO) prior to any travel. The frequencies of both requirements are not possible to predict, therefore, an estimated amount has not been established for training and travel.

C.7 **Period of Performance**

The performance period begins with date of 08/01/2021 and the end date is 07/31/2022.

C.8 **Place of Performance**

Work for this task order shall be performed off-site. The Contractor will not be required to be located, or to maintain a local office in the Atlanta, Georgia, area. However, if the Contractor is located in a distant geographical location, they will be required to schedule regular conference calls and travel to Atlanta for face-to-face meetings with the COR and End User as specified in the PWS to facilitate close working relationships with CDC's project staff.

C.9 **Government Furnished Property**

The government will provide contract personnel with an identification badge (HHS-576-CDC) and CDC cardkeys to gain entrance to designated CDC buildings and CDC user accounts (which consist of user IDs and passwords and are required to gain access to CDC LAN/WAN computer environments). Issuance of identification badges to contract personnel is contingent upon successful completion of a NACI or Federal investigative process as required in accordance with Homeland Security Presidential Directive-12 (HSPD-12). Government property including CDC computer equipment, keyfob, and blackberry if deemed necessary will be provided by NCIPC/DVP to perform assigned requirements.

C.10 **Deliverable(s) Schedule**

The contractor shall deliver, within the time frames specified, to the Contracting Officer's Representative (COR), at the address shown in Section G, and copies of items so specified, to the Contracting Officer at the address shown on the face page of the contract.

Deliverables

- **Daily Media Monitoring Newsletter** - A filtered and branded email updated with key media hits for each topic monitored. Delivered via email by 1pm Eastern each day the report is due.
- **Weekly Status Reports** – A dashboard of on-going activities with target completion dates, and details regarding current progress, known issues/delays, and other pertinent information.
- **Monthly Status Report** - A dashboard of on-going activities with target completion dates, and details regarding current progress, known issues/delays, and other pertinent information.
- **Monthly Media Dashboard** -The dashboard will be used to summarize monthly results from media outreach and engagement efforts. Insights will also inform changes and shifts in strategy.
- **Analysis and Evaluation Report for Media Outreach Effort** – A report for each effort is due 30 days after the media outreach effort. Key performance indicators and measure included in report to be reviewed and approved by CDC prior to implementation.

Performance Based Matrix

Performance-based Matrix				
Desired End Result	Feature(s) of end result to be surveilled (Standard).	Acceptable Quality Level (AQL).	Monitoring Method	Incentives/Payment-Quality Link
Consistently develops communication products that are timely, well written, and engaging.	Accuracy, Timeliness, and Customer Satisfaction	95% of products in accordance with outlined standards.	Services will be primarily customer observations.	Favorable or Unfavorable Performance Evaluation
Consistently provides responsive service to internal/external customers to support customer and program requirements.	Accuracy, Timeliness, and Customer Satisfaction	95% of all requests handled within 48 hours.	Services will be primarily customer observations.	Favorable or Unfavorable Performance Evaluation
Assigned tasks/projects are to be completed within established deadlines.	Accuracy, Timeliness, and Customer Satisfaction	95% of all requests handled within 48 hours.	Services will be primarily customer observations.	Favorable or Unfavorable Performance Evaluation
Completes all required reports and submits to the COR and other designated points of contact within NCIPC-	Accuracy, Timeliness, and Customer Satisfaction	Reports must be 95% - 100% accurate. Reports must be 100% on time	100% review of submitted reports.	Favorable or Unfavorable Performance Evaluation

OD by established deadlines. Complete weekly and monthly reports by agreed upon dates set between the COR and contractor.		addressing the requirements of C.4 Reporting Schedule		

C.11 **508 Help Desk**

HHSAR Provision, 352.239-74: Electronic and Information Technology Accessibility Notice

(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) supplies and services developed, acquired, or maintained under this contract or order must comply with the "Architectural and Transportation Barriers Compliance Board Electronic and Information Technology (EIT) Accessibility Standards" 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.hhs.gov/web/508. 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 or order are identified in the Statement of Work or Specification or Performance Work Statement. The contractor must provide any necessary updates to the submitted HHS Product Assessment Template(s) at the end of each contract or order exceeding the simplified acquisition threshold (see FAR 2.101) when the contract or order duration is one year or less. If it is determined by the Government that EIT supplies and services provided by the Contractor do not conform to the described accessibility standards in the contract, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(c) The Section 508 accessibility standards applicable to this contract are: 1194.

205 WCAG 2.0 Level A & AA Success Criteria
302 Functional Performance Criteria
502 Inoperability with Assistive Technology

504 Authoring Tools
602 Support Documentation
603 Support Services

(d) In the event of a modification(s) to this contract or order, which adds new EIT supplies or services or revises the type of, or specifications for, supplies or services, the Contracting Officer may require that the contractor submit a completed HHS Section 508 Product Assessment Template and any other additional information necessary to assist the Government in determining that the EIT supplies or services conform to 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 Web site: (http://hhs.gov/web/508). If it is determined by the Government that EIT supplies and services provided by the Contractor do not conform to the described accessibility standards in the contract, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(e) If this is an Indefinite Delivery contract, a Blanket Purchase Agreement or a Basic Ordering Agreement, the task/delivery order requests that include EIT supplies or services will define the specifications and accessibility standards for the order. In those cases, the Contractor may be required to provide a completed HHS Section 508 Product Assessment Template and any other additional information necessary to assist the Government in determining that the EIT supplies or services conform to Section S08 accessibility standards. Instructions for documenting accessibility via the HHS Section 508 Product Assessment Template may be found at http://hhs.gov/web/508. If it is determined by the Government that EIT supplies and services provided by the Contractor do not conform to the described accessibility standards in the provided documentation, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

C.12 **Severability Determination**

This is a severable services contract need.

C.13 **Contracting Officer's Representative (COR) responsible for this contract**:

Sarah Roby
Centers for Disease Control and Prevention (CDC)
4770 Buford Hwy, NE
Chamblee Building 106

Atlanta, GA 30341
Telephone Number: 404-498-1375
Email: mkq4@cdc.gov

C.14 **References**

The contractor shall have:

- Knowledge of internal/business communication practices
- Ability to communicate orally and in writing
- Strong organizational skills, attention to detail, and adherence to deadlines
- Ability to work in a fast-paced environment
- Experience working with senior leaders in an organization

INFORMATION 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 Categorizatian of Federal Information and Informatian Systems*, the Contractor (and/or any subcontractor) shall:

a. Protect 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 Informatian 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: N/A

Confidentiality:	[ ] Low [ ] Moderate [ ] High
Integrity:	[ ] Low [ ] Moderate [ ] High
Availability:	[ ] Low [ ] Moderate [ ] High

Overall Risk Level: [ ] Low [ ] 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: [X] Low [ ] 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 "*handling"* 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 ond Privacy Controls for Federol Informotion Systems ond Orgonizations* 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 protect its confidentiality, integrity, and/or availability. The Contractor (and/or any subcontractor) shall protect 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 and CDC policies. Unauthorized disclosure of information will be subject to the HHS/CDC 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 protect 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 and CDC-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 and ISSO within 30 days of contract award.

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 CDC non-disclosure agreement. 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 CDC 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 CDC SOP or designee with completing a PIA for the system or information within *30 days* 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 CDC 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.

B. 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/CDC 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 *CDC specific* 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 Respansibilities 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.

C. 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*, and any CDC-specific rules, as applicable.

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 CDC 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.

D. 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)/CDC CSIRT 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) Protect 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 CDC approved notifications to affected individuals following CDC's designated process.

3) Report all suspected and confirmed information security and privacy incidents and breaches to the CDC's Computer Security Incident Response Team (CSIRT) *[CSIRT@CDC.gov]*, COR, CO, CDC 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 CDC and 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 Infarmatian* HHS and CDC's 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.

E. 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 requiring activity representative, in conjunction with Personnel Security, shall use the OPM Position Sensitivity Designation automated tool (https://www.opm.gov/investigations/) to determine the sensitivity designation for background investigations. After making those determinations, include all applicable position sensitivity designations.

F. 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. For additional information, see HSPD-12 policy at:* https://www.dhs.gov/homeland-security-presidential-directive-12)

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 the CDC Specified timeline of the effective date of this contract. Any revisions to the roster as a result of staffing changes shall be submitted within 7 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.

G. Contract Initiation and Expiration

1) **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 CDC EPLC framework and methodology and in accordance with the HHS Contract Closeout Guide (2012). CDC EPLC requirements may be located here: https://www2a.CDC.gov/CDCup/library/other/eplc.htm.

2) **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.

3) **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 Sanitizatian*.

4) **Notification.** The Contractor (and/or any subcontractor) shall notify the CO and/or COR and system ISSO within 7 days before an employee stops working under this contract.

5) **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 CDC policies.

6) The Contractor (and/or any subcontractor) shall perform and document the actions identified in the CDC Contractor Employee Separation Checklist when an employee terminates work under this contract within 7 days of the employee's exit from the contract. All documentation shall be made available to the CO and/or COR upon request.

H. 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/CDC policies and shall not dispose of any records unless authorized by HHS/CDC.

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/CDC policies.

(End of provision)

AWARD/CONTRACT

1. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	RATING	PAGE OF PAGES
▶		1 | 61

2. CONTRACT (*Procurement, Instruction, Identification*) NUMBER	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQUEST/PROJECT NUMBER
75D30121C11737	08/13/2021	00HCVG1A-2021-59558

5. ISSUED BY	CODE	8219
Centers for Disease Control and Prevention (CDC) Office of Acquisition Services (OAS) 2900 Woodcock Blvd, MS TCU-4 Atlanta, GA 30341-4004		

6. ADMINISTERED BY (*If other than Item 5*)	CODE	8219
Centers for Disease Control and Prevention (CDC) Office of Acquisition Services (OAS) 2900 Woodcock Blvd, MS TCU-4 Atlanta, GA 30341-4004		

7. NAME AND ADDRESS OF CONTRACTOR (*Number, Street, County, State and ZIP Code*)	8. DELIVERY	9. DISCOUNT FOR PROMPT PAYMENT
SENSIS INC. 818 S BROADWAY ST STE 1100 LOS ANGELES, CA 90014-3249	☐ FOB ORIGIN ☒ OTHER (*See below*)	Net 30

CODE 003081689	FACILITY CODE	10. SUBMIT INVOICES (*4 copies unless otherwise specified*) TO THE ADDRESS SHOWN IN: ▶	ITEM

11. SHIP TO/MARK FOR	CODE	12. PAYMENT WILL BE MADE BY	CODE	434
		Centers for Disease Control and Prevention (FMO) PO Box 15580 404-718-8100 Atlanta, GA 30333-0080		

13. AUTHORITY FOR USING OTHER THAN FULL AND OPEN COMPETITION:	14. ACCOUNTING AND APPROPRIATION DATA
☐ 10 U.S.C. 2304(c)( ) ☒ 41 U.S.C. 3304(a)(2)	See Section B

15A. ITEM NUMBER	15B. SUPPLIES/SERVICES	15C. QUANTITY	15D. UNIT	15E. UNIT PRICE	15F. AMOUNT
	"See Section B"				

15G. TOTAL AMOUNT OF CONTRACT ➔ (b)(4)

16. TABLE OF CONTENTS

(X)	SECTION	DESCRIPTION	PAGE(S)	(X)	SECTION	DESCRIPTION	PAGE(S)
		PART I – THE SCHEDULE				*PART II – CONTRACT CLAUSES*	
X	A	SOLICITATION/CONTRACT FORM	1	X	I	CONTRACT CLAUSES	57
X	B	SUPPLIES OR SERVICES AND PRICES/COSTS	2			*PART III - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACHMENTS*	
X	C	DESCRIPTION/SPECS./WORK STATEMENT	4	X	J	LIST OF ATTACHMENTS	Error!
X	D	PACKAGING AND MARKING	37			*PART IV - REPRESENTATIONS AND INSTRUCTIONS*	
X	E	INSPECTION AND ACCEPTANCE	38		K	REPRESENTATIONS, CERTIFICATIONS AND OTHER STATEMENTS OF OFFERORS	
X	F	DELIVERIES OR PERFORMANCE	39				
X	G	CONTRACT ADMINISTRATION DATA	40		L	INSTRUCTIONS, CONDITIONS, AND NOTICES TO OFFERORS	
X	H	SPECIAL CONTRACT REQUIREMENTS	44		M	EVALUATION FACTORS FOR AWARD	

CONTRACTING OFFICER WILL COMPLETE ITEM 17 (SEALED-BID OR NEGOTIATED PROCUREMENT) OR 18 (SEALED-BID PROCUREMENT) AS APPLICABLE

17. ☒ CONTRACTOR'S NEGOTIATED AGREEMENT (*Contractor is required to sign this document and return* 1 *copies to issuing office.*)

Contractor agrees to furnish and deliver all items or perform all the services set forth or otherwise identified above and on any continuation sheets for the consideration stated herein. The rights and obligations of the parties to this contract shall be subject to and governed by the following documents: (a) this award/contract, (b) the solicitation, if any, and (c) such provisions, representations, certifications, and specifications, as are attached or incorporated by reference herein. (Attachments are listed herein.)

18. ☐ SEALED-BID AWARD (*Contractor is not required to sign this document.*)

Your bid on Solicitation Number 75D301-21-R-71975 including the additions or changes made by you which additions or changes are set forth in full above, is hereby accepted as to the terms listed above and on any continuation sheets. This award consummates the contract which consists of the following documents: (a) the Government's solicitation and your bid, and (b) this award/contract. No further contractual document is necessary. (Block 18 should be checked only when awarding a sealed-bid contract.)

19A. NAME AND TITLE OF SIGNER (*Type or print*)	20A. NAME OF CONTRACTING OFFICER
Robyn Loube, Vice President	Sarah Turner

19B. NAME OF CONTRACTOR	19C. DATE SIGNED	20B. UNITED STATES OF AMERICA	20C. DATE SIGNED
BY [signature] (*Signature of person authorized to sign*)	Sept. 10, 2021	BY Sarah H. Turner -S Digitally signed by Sarah H. Turner -S Date: 2021.09.10 17:00:52 -04'00' (*Signature of Contracting Officer*)	

AUTHORIZED FOR LOCAL REPRODUCTION
Previous edition is NOT usable

STANDARD FORM 26 (REV. 3/2013)
Prescribed by GSA - FAR (48 CFR) 53.214(a)

Sensis Inc.: Robyn Loube, (b)(6)
CDC COR: Cate Shockey, gqw6@cdc.gov, 404.639.5028
CDC Contract Specialist: Sarah Turner, kwp9@cdc.gov, 404-498-5613

"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 B - Supplies Or Services and Prices/Costs

ITEM	SUPPLIES / SERVICES	QTY / UNIT	UNIT PRICE	NOT TO EXCEED
0001	COVID Vaccine & Travel Support Comprehensive communication services to support travel campaign efforts for target audiences. See Statemnet of Work ERR 20-15-5088; 20-15-6420 Period of Performance: 8/13/2021 – 8/12/2022 Time & Materials Line Item Non-Severable Services Monthly invoicing in arrears	(b)(4)		
	Line(s) Of Accounting: 9390EX2 2512 2021 75-2024-0943 C323111101 (b)(4) 9390GLZ 2512 2021 75-2124-0943 C5B8111101 (b)(4)			

Note: Authorizations to Proceed were issued via e-mail by Contracting Officer Sarah Turner on August 13, 2021

B.1 LABOR CHART

LABOR CATEGORY & ESTIMATED LEVEL OF EFFORT				
Line Item	**Estimated Labor Category**	**Hourly Rate (fully burdened)**	**Estimated Level of Effort**	**Estimated Labor Cost**
001	Project Director	(b)(4)		
001	Account Supervisor			
001	Senior Account Executive			
001	Account Executive			
001	Account Coordinator			
001	Health Communications Specialist			
001	Social Media Manager			
001	Creative Director/Art Director			
001	Associate Creative Director			
001	Motion Graphic Designer			
001	Copywriter			
001	Sr. Copywriter			
001	Media Director			
001	Media Supervisor			
001	Media Planner/Buyer			
001	Analytics Manager			
001	Strategy Director			
001	Strategist			
TOTAL				

NOTATION REGARDING LABOR HOUR VARIANCE: Performance under this Time and Materials/Labor Hour Contract is in accordance with FAR 52.232-7, "Payments under Time and Materials and Labor Hour Contracts," incorporated by reference in Section I, which requires the vendor to manage to the ceiling price in the contract and the ceiling price of the line items. The number of hours per labor category are estimates. The CO and the COR must be notified of any variance from the estimated hours shown in the Level of Effort/Labor Categories chart.

Section C - Description/Specification/Work Statement

Performance Work Statement
Title: COVID-19 Vaccine and Communication Support

SECTION 1 – BACKGROUND
CDC Travelers' Health Branch provides health information to travelers, including specific vaccine, disease, and health advice for destinations around the world. In the midst of the COVID-19 pandemic, Travelers' Health has focused on providing domestic and international travel health information and recommendations to help travelers protect themselves, their loved ones, and their communities. As COVID-19 vaccines become more widely available in the United States, travel messaging and recommendations will become even more complex and important.

As vaccination rates increase and summer travel season arrives consumer polling shows most demographic and age groups are reporting an increased interest in travel. CDC Travelers' Health is planning a multipronged communication effort to target key audiences including but not limited to baby boomers (people 65+), a segment of Millennials (35-40), and Gen X travelers (people 41-54 years old), as well racial and ethnic minority populations and vaccine hesitant travelers identified within these age groups. Services will include message development and testing; partner identification and outreach; web content, audiovisual, and graphic development; paid ads; and media and partner toolkits.

SECTION 2 – PURPOSE
Since travel increases an individual's chances of getting and spreading COVID-19, these campaign efforts will focus on providing target audiences the information they need to get vaccinated before travel as well as protect themselves and loved ones before, during, and after travel over the next 8-10 months, regardless of vaccine status.

The proposed contract covers comprehensive communication services to support campaign development and execution including audience assessment, message development, testing, and evaluation, partner identification and engagement, media relations, and product development and delivery. The goal of these efforts is to effectively reach domestic and international travelers with clear, actionable, and accessible COVID-19 travel health information to motivate travelers to protect themselves, their loved ones, and the communities in which they live and travel, including vaccination.

SECTION 3 – SCOPE OF WORK
The proposed contract covers comprehensive communication services to support travel campaign efforts for target audiences. These services include all facets of campaign development and execution including audience assessment, message development, testing and evaluation, partner identification and engagement, media relations, and product development and delivery.

The contract will include the following scope of services:

1) Formative, Concept and Message/Materials Testing: The contractor will conduct audience assessments as needed and provide data on target audiences' knowledge, attitudes, and practices related to travel (including travel planning, risk and protective behaviors, and motivators and barriers to protective behaviors) to guide product development and implementation. The vendor will also conduct materials and message testing to determine efficacy. Assessments will include rapid assessments to regularly evaluate messages, channels and products posted on CDC's dissemination channels.

2) Communication Strategy: The contractor will develop, refine, and update a communication strategy and plan, building on audience assessments and marketing insights, that will identify effective platforms and drive message reach, receptivity and behavior change to meet objectives. Strategy will include media buying plans and partnership development.

3) Product Development: The contractor will develop messages and materials to achieve goals, based on findings from audience assessments and marketing insights. These will include ads for television, print, radio, out-of-home, and digital channels (among others identified through assessments) for both national and local placement.

4) **Partner Identification and Engagement:** The contractor will assist CDC's Travelers' Health Branch with strengthening existing partnerships as well as identifying new partnerships and relationships for CDC to pursue with influencers, bloggers, travel companies, etc. These efforts will increase reach beyond CDC platforms and help ensure that content is delivered in an appropriate and culturally competent manner.

5) Graphic Design: The contractor will provide graphic design services (including packaging for paid and unpaid ads and the development/acquisition of graphics, illustrations, drawings, photographs, slides, and other similar visual materials) ensuring CDC standards are followed.

6) Distribution: Paid and Non-paid Ad, Media, and Social Media: The contractor will develop and implement a media distribution plan that will include paid and non-paid media opportunities, including a comprehensive media and social media strategy, recommendations, materials, tools, and resources to promote and enhance the reach and attention to resources and digital assets, such as the website, through the use of various platforms.

7) Process and Outcome Evaluations: The contractor will develop and execute process and outcome evaluation plans to assess campaign reach and impact. At a minimum, contractor should gather feedback on dissemination and reach of all materials, including partner materials, utilizing a variety of metrics, and will provide a routine metrics report that includes opportunities to further strengthen reach and awareness. Contractor should also assess audience awareness of and reactions to the campaign, as well as campaign impact on intended audiences' COVID-19 knowledge, attitudes, and vaccine and travel behaviors.

SECTION 4 – TASKS TO BE PERFORMED

TASK 1: Formative, Concept and Message Testing

The contractor will develop and execute a plan to conduct formative assessments and message/materials testing with a variety of audiences. The contractor will need to move swiftly; rapid and real-time feedback mechanisms should be incorporated into the plan.

A thorough understanding of the target audiences and the barriers and motivators associated with a specific call to action is essential. This understanding will facilitate the development of messages and materials, inform the placement of media, and enhance the communication strategies and tactics that resonate with target audiences. Priority target audiences may shift as the pandemic evolves and travel behaviors shift. Currently they include but are not limited to baby boomers (people 65+), a segment of Millennials (35-40) and Gen X travelers (people 41-54 years old), as well racial and ethnic minority populations and vaccine hesitant travelers identified within these age groups. Contractors will use most effective and appropriate methodologies and behavior change theory to develop strategic recommendations that guide the development of these communication activities.

1.1 **Review prior applicable marketing insights and develop testing methodologies**

The contractor will use prior formative work from related health communications and educational efforts, including any applicable audience or marketing insights collected or reviewed by CDC. The contractor will develop a technical plan with recommended rapid, cost-effective and appropriate methodologies to conduct formative assessments and to test concepts, messages, and products.

1.2 **Conduct formative, concept and message/materials testing**

To guide message, material, and creative development, the contractor will review and conduct formative assessments with target audiences to gauge knowledge, attitudes, beliefs, practices and communication preferences. This will include gaining insights into individual, interpersonal and cultural motivators and barriers to engaging in recommended protective behaviors before, during and after travel; values related to travel and COVID-19 prevention; trusted COVID-19 and travel information sources; and effective communications channels. Contractor will provide summary reports with recommendations for communication strategies, including additional audience segmentation (if needed), channels, sources, messaging (content, appeal, tone, creative), and materials.

Contractor will conduct concept, message, and materials testing to gauge audience attention and comprehension, as well as content relevance, appropriateness, and effectiveness. The contractor will implement a comprehensive approach for testing all proposed messages and materials using rapid testing and analysis. If languages in addition to

English are identified as necessary to reach and meet the needs of identified target populations then identified messages and materials will be tested in those languages. The contractor will provide message/materials testing reports with key findings and recommendations, and revise concepts, messaging and materials based on findings.

Contractor shall develop audience recruitment, screening, and data collection tools. De-identified data files for all phases of audience assessments should be shared with CDC.

1.3 **Data support**
The contractor will provide CDC with summary reports containing findings and recommendations for communication strategy for effectively reaching priority audiences.

1.3.1 **Publications and presentations**: In coordination and consultation with the CDC's Technical Monitor and other project staff, manuscripts and/or presentations will be developed by the contractor regarding assessment results and analyses.

1.3.2 **IRB and/or OMB package submissions**
In coordination and consultation with CDC staff, the contractor will prepare the Human Subjects Review and Office of Management and Budget (OMB) determination and clearance packages for data collection. The contractor will provide all the applicable information necessary for the IRB/OMB packages, including screen shots of online testing surveys or moderator guides, information about privacy and informed consent, compensation, and recruitment methods.

TASK 2: Develop a Communication Strategy

The contractor shall:
a) The contractor will develop, refine, and update a communication strategy and plan, building on the formative assessments, that will drive behavior change and will result in met objectives. This should include plans to:

1. Assess messaging gaps and opportunities, including refreshing existing CDC materials/messaging and developing new messages and materials.
2. Reach priority audiences through effective messaging, platforms, design, images, sources, and channels.
3. Leverage all CDC communication platforms and distribution networks of partner organizations, as well as new paid and unpaid channels for reaching intended audiences.

The plan will provide expert recommendations for how to tailor messaging, creative concepts, and outreach strategies to best reach and accomplish objectives for each communication audience.
The communication plan will describe all contract activities in detail and will include measurable objectives and plans to evaluate them. This plan will allow for flexibility both in priorities and content as new issues concerning travel evolve, but should also provide schedules and details such as drafts, revisions, clearance, additional revisions, finals, and delivery to CDC.

The contractor will develop a media buying plan, based on findings of audience assessments and marketing insights and identified priority target audiences. This may include distribution through digital, trade, traditional media, and other channels with effective reach among target audiences. All materials will need to take into account target audiences' various cultures, languages, and trusted sources of information.

TASK 3: Product Development

The contractor will apply audience and marketing findings to develop campaign products and materials. The contractor will use their best approach for managing creative material production with multiple audience segments and possible translation of materials if and as needed.

3.1 **Product development**

The contractor shall develop a set of interrelated materials (based on and tested during the assessment phase) for identified target audiences. Materials should have a consistent creative concept, look, and theme and in accordance with Task 5 specifications.

a) The suite of materials might include, but is not limited to:

1. Videos and audio podcasts that can be posted on CDC and partner websites
2. Digital ads (formatted for multiple platforms, such as Google search, Google Display Network, YouTube, and point of purchase ads)
3. Partner letters & toolkits
    a. Federal Partners
    b. Private partner and influencer/blog toolkits
    c. Media toolkits
4. Media tailored content (e.g., shareable images, quizzes, or engagement resources)
5. Traditional media advertisements (television, print, radio)
6. Social media content and ads
7. Blog posts or related digital content co-written with influencers and bloggers

Materials and strategies should be developed to specifically address audience subsets. The contractor shall test materials with identified audiences to ensure materials are successfully received, as noted in Task 1.2.

3.2 **Media asset inventory**

The contractor will develop an inventory of all materials developed throughout the duration of the performance period. The media asset inventory will be updated as needed, but at least monthly. The contractor will ensure that a naming convention is established and is reflected in the media asset inventory.

3.4 **Logos/tagging, captioning, audio podcast development**

3.4.1 **Logos/tagging:** All materials developed will be tagged with HHS and CDC logos and/or Web site URLs. The contractor must adhere to the CDC and COVID-19 branding and style guides.

3.4.2 **Captioning and Audio Description**: In addition to compliance of Section 508 (described in more detail after task 7), any videos produced by the contractor as part of this contract will be closed captioned and audio described using software that is compatible with CDC servers. All caption files will be turned over to CDC once captioning and audio description is complete. The contractor will also follow CDC best practices for closed captioning. This information can be found at the following URL: https://www.hhs.gov/web/section-508/making-files-accessible/index.html

3.4.3 **Audio Podcast Development:** Any video produced by the contractor will have an accompanying podcast that provides a spoken description of the visual elements, along with the original audio elements. This will ensure compliance with Section 508 and provides the opportunity for people who are visually impaired to understand all elements (visual and audio) of the original video. Work associated with this task will include preparing stand-alone audio files, creating narrative scripts that describe visual elements, recording narrative scripts and integrating them into the videos' audio files, preparing the final audio products (podcasts), and creating collateral content such as transcripts and summary descriptions. Once completed, all audio description files will be shared with CDC for approval.

3.5 **Clearance and Government Regulations/Formats**

The contractor shall follow all CDC clearance, branding, and web compliance requirements when creating educational resources. The contractor shall:

1. Obtain feedback on materials, target audiences, and specific stakeholders; refine materials based on feedback.
2. Submit all materials to CDC for clearance and incorporate CDC clearance into timelines.
3. Ensure all materials follow CDC web requirements and are 508 compliant
4. Provide editable versions of all materials and graphic elements.

All draft and prototype materials will be submitted for review and approval by CDC before they are finalized for printing, duplication, or distribution.

The contractor will follow all required HHS and CDC clearance requirements and procedures. The contractor will use **Adobe Creative Cloud** to produce materials and products. Print materials will be created in accordance with Government Printing Office (GPO) rules and regulations https://www.govinfo.gov/features/new-edition-gpo-style-manual. All materials prepared for television, print, digital and radio must be in a format that is appropriate for Internet use, including meeting Section 508 compliant requirements.

HHS policy requires that health-related media products receive approval from the Office of the Assistant Secretary for Public Affairs (ASPA) before release to the public. The contractor will complete the necessary form(s) for Strategic Communications Portal submission, the mechanism by which CDC requests ASPA review and clearance of new materials. The form will be shared during the kick-off meeting.

TASK 4: Partner Identification and Engagement

The contractor will assist Travelers' Health with strengthening existing partnerships as well as identifying new partnerships and relationships for CDC to pursue with influencers, bloggers, travel companies, etc. These efforts will increase reach beyond CDC platforms and help ensure that content is delivered in an appropriate and culturally competent manner. CDC will be the main driver in partnership outreach and communication.

4.1 Strengthen existing partnerships
Contractor will strengthen existing partnership with federal and private partners through collaborative (pro-bono) or paid content development, including toolkits with resources and visual elements that partners can use to reach key audiences through their channels.

4.2 Identify new partnerships
Contractor will identify new partnerships for CDC to pursue that will help expand the reach of these communication efforts and offer opportunities for ongoing/long-term partnerships for CDC's Travelers' Health Branch.

4.3 Develop Partnership Agreements
When necessary, contractor will develop a partnership agreement that clearly define CDC's and the partner's roles and responsibilities.

TASK 5: Graphic Design, Photos, Layout, and Support

5.1 The contractor will provide graphic design services (including packaging for public service announcements and the development/acquisition of graphics, illustrations, drawings, photographs, slides, etc.) ensuring CDC standards are followed.

5.1.1 **Specifications/requirements**
Any photographs, other artwork, or animations used by the contractor must be royalty free/copyright free, digital at a resolution of 300 dpi, and at a width of 20 inches when possible (poster quality). The contractor will arrange for a buyout for CDC of the photo, artwork, or animated images and acquire them without limitations of use. Photos must be able to be used on social media platforms (including Facebook, Twitter, Instagram, and LinkedIn) and on CDC Web sites. 5.1.2 **Original artwork**
The contractor will be required to develop original artwork (for print, web, and/or social media platforms) or animation (in the form of GIFs and MP4). All original artwork or animations created for this project will become the property of CDC with full and unlimited rights transferred.

5.1.3 **Software**
Electronic prepress files furnished for printing will be created using Mac OS X or later or Microsoft Windows XP Professional or later using recordable CD or DVD media and secure electronic file transfer, using the following software: page layout– Adobe InDesign; drawing/illustration–Adobe Illustrator; image manipulation–Adobe

Photoshop. The contractor will use software in correct native format, latest version, and without third party extensions/plugins.

5.1.4 **Desktop publishing and print production**
All desktop publishing must be completed using the latest version of Adobe InDesign software to include Adobe Illustrator and Adobe Photoshop. All graphic design must be completed using Adobe Creative Cloud software. Also, print media files will include all images and fonts used. Fonts will be Postscript or Open Type ONLY. Images will be CMYK, grayscale, and duotone (NOT RGB). In addition to CD/DVD and secure electronic file, the contractor will furnish a press-quality PDF as well as a laser print (in color as required) hard copy of final file. Files for CDC print materials will be press-ready, such as passed through a program such as "Flight Check." Note: the contractor must either use fonts CDC owns or purchase them without limitations of use for CDC. If stock photos are used or must be purchased, the contractor must assign the license to CDC or purchase them without limitations of use by CDC. The contractor will provide 508-compliant PDFs of final graphic products.

5.1.5 **Image catalog/listing**
The contractor will provide a comprehensive table listing sources of images, location of images (if included in a brochure), and description of usage rights.

TASK 6: Distribution: Paid and Non-paid Ads, Media & Social Media
The contractor will develop and manage a comprehensive media buying plan as described below and mentioned in Task 2 that will integrate into and support the communication strategy. The plan should include opportunities for paid and non-paid media placement, focusing on educational opportunities to reach target audiences. Once the media plan is approved by the government, the contractor will manage the media buying process and make direct placement of ads and sponsorships. The contractor will also measure the reach and impact of the media placements and social media tactics against key performance indicators.

Media buys will include digital, social, trade, and traditional media targeting identified target populations. All materials will need to take into account each targeted group and subgroup's various cultures, languages, and trusted sources of information.

Distribution strategies will include paid media placement and other digital and social media distribution platforms such as Point of Purchase on partner and paid travel booking sites, Facebook, Twitter, Pinterest, Instagram, LinkedIn, and other platforms recommended by the contractor based on consumer and marketing insights.

6.1 **Media Distribution and Paid Placement**

The contractor will provide support for direct paid media placement (e.g., digital, social media, print, outdoor, out-of-home, point-of-purchase); non-paid, in-kind or donated media placement, such as the placement of television or radio public service announcements and distribution of social media content; and support for other public health marketing activities.

6.2 **Engagement Tactics**

6.2.1 Develop original, creative, unique, branded images and GIFs

The contractor will:

a) Develop branded images and/or GIFs.
b) Develop original images that deliver key messages and resources, deepen understanding about priority groups, COVID-19 vaccine, and encourage fans to share images/messages.
c) Images can be developed by using or modifying stock photography and illustrations, as appropriate.
d) Images can be used to enhance other engagement strategies.

6.2.2 Amplify content on other social media platforms

a) The contractor will identify opportunities to share messages across CDC's available social media accounts by providing posts that cross-promote messages from CDC's main Facebook, Twitter, Instagram, LinkedIn, and Pinterest accounts, as appropriate for those channels, content strategies, and audiences.
b) Conduct outreach to bloggers, other influencers and engage them to write about the topic areas and cross-promote CDC content.
c) Promote relevant hashtags across social media accounts.

6.2.3 Create compelling, visually stimulating videos optimized for social media

a) The contractor will develop creative brief for videos.

b) Draft pre-production and pre-release CDC OADC clearance forms, as needed.

c) Create storyboards for videos.

d) Develop scripts/transcripts, if necessary.

e) Create original graphics, stage photos showing diverse people in different settings, and secure trusted spokespersons for the videos.

f) Ensure videos are 508 compliant; this includes captioning and audio description files.

g) HHS policy requires that health-related media products receive approval from the Office of the Assistant Secretary for Public Affairs before release to the public. As required and at the COR's direction, the Contractor will submit the necessary clearance packages to the COR, which will include required forms and supporting materials (e.g., storyboards). Required forms will be completed in accordance with the HHS Public Affairs Management Manual (HHS Transmittal 86.01, issue date 11/21/86). The package must be approved before final copy or production can be initiated. At the COR's direction, the contractor will prepare presentations on or attend meetings to discuss the materials or the clearance package. The contractor will incorporate changes as directed by Government review.

6.3 **Digital Media Planning**

The contractor will provide a full range of digital media planning capabilities for a variety of audiences. The contractor will develop and submit a digital media marketing plan as mentioned in Task 2 which will include:

a) The background and rationale for the plan;

b) Overall goals and SMART (Specific, Measurable, Achievable, Relevant, and Time-Bound) communication objectives;

c) a description of each of the tactics being proposed, such as but not limited to digital display ads, badges, and buttons, digital video (organic and ads), and paid search;

d) a profile of primary audience (as requested by CDC) and potential motivations, influences, exchanges, and benefits and barriers of desired behavior for each;

e) a delivery schedule to include all tactics (which anticipates lead times to develop, technically review, test, obtain approvals, and produce in final copy all such materials needed for implementation);

f) a description of the evaluation approach and proposed methods (ensure evaluation approach is consistent for comparison purposes) for evaluation reports to gauge progress, determine forward direction, and implement necessary changes and updates accordingly;

g) a discussion of any negative, unintended consequences to avoid.

6.4 **Web-based strategies**

The contractor may create content and graphics to support the deployment of content for the website, including content for mobile and RSS/Syndication. Creative pieces must meet CDC and HHS web standards in order to be posted on CDC.gov websites and databases (such as Media Campaign Resource Center (MCRC) and the Publications Catalogue and Ordering System) and included on CDC's YouTube channel for CDC.gov website streaming. All creative assets need to be available for incorporation in CDC.gov platforms as needed and requested by COR. All content will be Section 508 compliant (described in detail below the description of work section) and will be designed to optimize the user's experience across digital platforms, including the growing number of mobile/device users. This content includes pdfs, badges, buttons, banners, html, xml, and css content. Familiarity with CDC templates and the CDC development environment, especially the Web Content Management System.

6.5 **Evaluate Engagement Tactics**

The contractor will track and assess performance through routine social media metrics reports that evaluate quantitative results and draw qualitative findings to track progress toward annual goals and objectives.

a. Reports should feature a narrative, visuals, comparisons of data over time, and recommendations to improve and enhance content, strategies, and outreach.

1. Present impact/metrics reports to track coverage, placement, and value of these activities.

2. Use metrics and trend spotting to continually refine the outreach strategy.

6.6 **Social Media Recommendations**

The contractor will recommend new ideas for engagement tactics based on analysis of metrics and evaluation data. The contractor will assess the strengths and weaknesses of the tactics and will make formal, written recommendations to the COR for future improvements.

6.7 **Digital Media Recommendations**
The contractor will develop written recommendations regarding what digital media tools, applications, platforms, channels should be used to engage users in the communication activities. Recommendations will be incorporated/presented in monthly digital media reports for consideration before inclusion in a digital media plan. The contractor will provide data/marketing insights supporting the tactics and provide data supporting the use of each recommended channel/tool/platform, as requested by the COR.

The contractor will develop the digital media recommendations and plans in accordance with CDC's Social Media Guidance and Tools—http://www.cdc.gov/SocialMedia/Tools/guidelines/.

TASK 7: Process and Outcome Evaluations

Contractor shall implement process and outcome evaluations of this communication effort, allowing for mid-course check-ins and strategic redirection, as the COVID-19 response evolves and audience and messaging needs change.

The contractor will track and gather feedback on dissemination and reach of materials, including partner materials, utilizing a variety of metrics, and will provide a routine metrics report that includes opportunities to further strengthen reach and awareness. The contractor will also assess audience awareness of the campaign, as well as campaign impact on intended audiences' COVID-19 knowledge, attitudes, and travel behaviors.

7.1. **Process evaluation**

Process evaluation should include tracking of program implementation, reach and uptake to allow optimization and strategic redirection as needed. For example, contractor should monitor progress to assess effectiveness of strategies/approach and make recommendations for modifying the plan when appropriate. Iterative message/product testing may also be needed. Community listening sessions, crowd-sourced surveys, and online group discussions may be considered among other appropriate, cost-effective, and rapid turn-around methodologies. Efforts should assess information or other gaps in messaging and potential unintended effects.

Contractor shall develop audience recruitment, screening, and data collection tools. The contractor shall submit evaluation reports with clear recommendations for revisions or adjustments to communication strategies, as approved in the evaluation plan.

Contractor will conduct ongoing social listening to help CDC understand changes in public sentiment on issues related to vaccination and travel.

7.2. **Outcome evaluation**

Outcome evaluation should include assessments of audience awareness and response to the communication program, and behavioral or health outcomes, to the extent possible.

Contractor shall use appropriate methodology for culturally diverse audiences and relevant audience segments. Contractor shall develop audience recruitment, screening, and data collection tools. Data collections should be conducted in the target audiences' preferred language(s), as appropriate.

SECTION 5 – GOVERNMENT FURNISHED MATERIALS
There will be no Government Furnished Materials.

SECTION 6 – PERIOD OF PERFORMANCE / PLACE OF PERFORMANCE
POP: One year from the date of contract award
Place of Performance will be at the Contractor's facility and/or virtually

SECTION 7 – DELIVERABLES/REPORTING SCHEDULE

The Contractor shall be responsible for delivering all end items specified as follows:

Deliverable	Description/Quantity/Format	Due Date/Frequency	Receiver of Deliverable
TASK 1 – Formative, Concept and Message/Materials Testing			
Message platform testing	The contractor will conduct message testing for up to 10 message platforms (e.g., digital, social media, web) using Focus Groups, in-depth interviews (IDIs), surveys, or other appropriate methodologies.	Ongoing	Technical Officer
Materials testing	The contractor will develop creative concept testing for approximately 25 products, using Focus Groups, IDIs, surveys or other appropriate methodologies.	Ongoing	Technical Officer
Formative Assessments	The contractor will perform formative assessments with up to 6 priority audiences, using Focus Groups, IDIs, or other surveys or other appropriate methodologies.	Within 6 weeks of award	Technical Officer

Message platform testing report	The contractor will develop one message platform testing report to include the following sections: executive summary, introduction, methodology, results, conclusions, and any appendices.	Report is due two weeks following completion of message platform testing.	Technical Officer
Creative concept testing report	The contractor will develop one creative concept testing report to include the following sections: executive summary, introduction, methodology, results, conclusions, and any appendices.	Report is due two weeks following completion of creative concept testing.	Technical Officer
Assessment reports	The contractor will develop one final PowerPoint deck and one final report in Word to display the results. Both will contain final data.	Final PowerPoint deck is due one week after data collection ends; the final report in Word is due two weeks after data collection ends	Technical Officer
Publications and presentations	The contractor will develop manuscripts in Word and at least ten (10) presentations in PowerPoint regarding formative assessment results and other testing and analyses.	PowerPoint presentations are expected each performance period. Manuscripts are ongoing; as needed.	Technical Officer
IRB / OMB package submissions	The contractor will prepare the Human Subjects determination and/or Office of Management and Budget (OMB) clearance packages for each data collection activity. The contractor will use Acrobat 9.0 and higher for file compression of all OMB clearance packages.	Ongoing; as needed	Technical Officer
TASK 2— Develop a Communication Strategy and Plan			
Communication Strategy and Plan	The contractor will develop and submit a communication strategy and plan in Word providing a comprehensive description of all activities. Communication Strategy should include media buying plan.	Detailed outline due: 10 days after the PoP begins; Draft due: 15 days after receiving comments on outline; Final version due within 7 days after receiving revisions	Technical Officer
TASK 3- Campaign Product Development			

Target audience profiles	The contractor will include and submit target audience profiles for at least 5 audience profiles (e.g., people aged 35-54 years, people 65+, BIPOC audiences, vaccine hesitant audiences) in PowerPoint format for each target audience per communication objective.	Within 6 weeks of award	Technical Officer
Educational and Awareness Materials	The contractor will develop a suite of materials including: Videos and audio podcasts that can be posted on CDC and partner websites and promoted by partners Digital media tailored content (e.g., apps, shareable images, quizzes or engagement resources) Advertisements and public service announcements Type and quantity of materials will be determined annually based on approval of the communication plan.	Final creative materials due 15 days prior to communications activity launch.	Technical Officer
MCRC submission report	The contractor will submit a report in Excel that details the transfer all materials to the Media Campaign Resource Center, including confirmation that all appropriate talent releases and licensing agreements for any talent that appears in the produced materials (TV, radio, print, and Web) have been secured	At least 15 days prior to communication activities launch.	Technical Officer
Media Asset Inventory	The contractor will keep an inventory throughout the duration of the project of all media assets of each year of the communications project upon completion. The media asset inventory should be in Word format. This will be forwarded to CDC upon request.	On-going with a minimum annual requirement.	Technical Officer

Audio Podcast	Related to compliance with Section 508, for any video produced by the contractor as part of this contact, the contractor will develop a podcast in a MP3 or a MP4 format that provides a spoken description of the visual elements, along with the original audio elements. The podcast should include a transcript in Word format.	Concurrent delivery with each corresponding video	Technical Officer
TASK 4- Partner Identification and Engagement			
Plan to strengthen current partnerships	CDC will provide a list of current partners, contractor will develop a plan how campaign activities can strengthen partnership that outlines activities, timeline, and products.	Within 6 weeks of award	Technical Officer
New partnerships plan	Contractor will provide CDC with a plan for potential new partnerships that outlines a strategy for identifying and prioritizing partners, and strengths and opportunities of the partnership for the current campaign efforts as well as future possibilities.	Within 6 weeks of award	Technical Officer
Develop partnership agreements	Contractor will develop partnership agreements that clearly define CDC and partners roles and responsibilities for review.	Ongoing, as needed	Technical Officer
TASK 5 – Graphic Design, Photos, Layouts, and Support			
Image catalog/ listing	Provide a comprehensive table in Excel listing sources of images, thumbnail of image, use location of images (i.e., if included in a brochure) and description of usage rights.	Ongoing Final due 45 days prior to performance period end.	Technical Officer
TASK 6— Distribution: Paid and Non-paid Media & Social Media			
Paid Media Placement	Contractor will directly secure paid media placements in digital, social, trade, and traditional media (including Facebook, Twitter, and other social media platforms; trade publication media buys and sponsorships; and paid opportunities.		
Content calendars	The contractor will create monthly content calendars that propose at least 3-4 posts per week, as appropriate.	Monthly	Technical Officer
Images and GIFs	The contractor will develop up to 20 creative and unique COVID-19 social media branded images and/or GIFs per month, as part of the monthly planning process. Jpeg or GIF, and InDesign files to be delivered to CDC. Images provided in various sizes appropriate to the social media platform it will be used on.	Monthly	Technical Officer

Instagram Story creative briefs	The contractor will develop at least 12 CDC.gov Instagram story creative briefs in Word format (template to be shared upon award).	4- 6 weeks in advance of story placement	Technical Officer
Instagram stories	The contractor will submit at least 12 draft and final CDC.GOV Instagram story content that needs no more than two rounds of edits. Format is jpeg, GIF, or mp4 depending on creative brief.	Monthly	Technical Officer
Social media videos	The contractor will create at least 10 fifteen second or less videos. Following the process outlined above.	Monthly	Technical Officer
Create compelling, visually stimulating videos optimized for social media	The contractor will create up to 8 thirty second videos. Following the process outlined above.	Monthly	Technical Officer
Create compelling, visually stimulating videos optimized for social media	The contractor will create up to 8 one-minute videos for social media. Following the process outlined above.	Monthly	Technical Officer
Social Media Metrics reports and dashbaord	The contractor will document social media performance through development of monthly, biannual, and yearly social media metrics reports that evaluate quantitative results and draw qualitative findings to track progress toward annual goals and objectives. Format is PPT and template to be provided upon award.	Ongoing on a dashboard, monthly reports to share with stakeholder.	Technical Officer
Paid search key words and ad text document	On an monthly basis, the contractor will review and propose revisions to the Paid Search Buy as needed or requested to the following: English and Spanish keywords, ad groups, tagged URLs, ad text and Ad extensions (such as, but not limited to, click to call, messaging extension, and app download). The formatted template will be shared upon contract award.	Monthly	Technical Officer
Paid search dashboard	Contractor will develop a paid search dashboard and provide CDC with access to the dashboard.	By start of communications activity – staff should have access to online dashboard and access maintained throughout the paid search buy	Technical Officer

Monitoring, tracking, and reporting methods document	The contractor will develop a document that proposes methods to correlate, analyze and report on tracking and monitoring activities and, with CDC's approval, initiate monitoring and regular reporting on the success of these efforts. Ongoing if part of a dashboard or Format Word Doc.	Ongoing if part of a dashboard or 20 days of the start of PoP	Technical Officer
Monitoring reports	The contractor will submit a weekly monitoring report to ensure activities are going well and any adjustments can be made quickly. Format TBD within first 30 days of the start of the PoP.	Weekly during first month of communication activity and ongoing as digital/social media activities start.	Technical Officer
Tracking, report	The contractor will develop monthly tracking reports for all digital media activities in Word or Excel format.	Weekly reports on digital/social media performance should be provided within 5 business days of the end of each four-week interval. And as requested by COR.	Technical Officer
TASK 7 – Tracking and Analysis - Metrics and Refinement			
Meeting reports	The contractor will coordinate and facilitate bi-weekly conference call meetings with contractors and CDC staff on tasks and provide notes in Word from those meetings within 24 hours.	At least once per week; Meeting notes are to be delivered within 24 hours of the meeting.	Technical Officer
Meeting agendas	The contractor will coordinate and facilitate meetings with CDC staff at least once a week (more often, if needed) and will develop an agenda at least 24 hours prior to the meeting.	At least once per week; Meeting agendas are to be delivered at least 24 hours prior to the meeting.	Technical Officer
Monthly progress reports	The contractor will provide written monthly progress reports with information about progress toward activities, goals and objectives, promotional activities, and any obstacles or issues that must be addressed so that work proceeds on schedule. The contractor must immediately bring any delays in schedule to the COR's attention and not rely on routine communication, e.g., weekly reports. This report will also describe how much of the budget has been spent that month, how much has been obligated, and the remaining balance of funds and should be submitted with monthly invoices.	Monthly; the progress reports will be submitted with the contractor invoices	Technical Officer

Performance period end reports	The contractor will prepare reports in Word (samples available upon award) with all materials, reports, and electronic files documenting the major milestones, hurdles, and lessons learned during the period of performance. The contractor will include these reports on an encrypted hard drive.	10 days prior to end of the PoP	Technical Officer
Metrics reports	The contractor will develop at least 6 metrics reports (per performance period). These reports will be shared internally and with partners to keep them abreast of the. Drafts will be in Word and final documents will be in PDF for dissemination.	As needed	Technical Officer
Fiual Report		First draft submitted within 3 weeks of the end of the performance period.	Technical Officer

SECTION 8 – PERFORMANCE MATRIX

Deliverable or Service required	Performance Stander	Acceptable Quality Level (AQL)	Method of Surveillance	Incentives/Disincentives
TASK 1 – Monthly report	**Timeliness**	98% Monthly report is submitted timely by the scheduled due date; respond to all inquiries from the COR and technical monitor within one business day of receipt.	Review Final Report by COR and technical monitor.	Performance positive or negative will be noted on the Contractor Performance Assessment Reporting System (CPARS).
	Quality	100% of all tasks and products are executed, performed, and completed to the standard described in the requirement; reports demonstrate effective analysis and supported conclusions/ recommendations. Documents returned no more than one time for rework		
TASK 2 – Monthly report	**Timeliness**	98% Monthly report is submitted timely by the scheduled due date; respond to all inquiries from the	Review Final Report by COR and	Performance positive or negative will be noted on the Contractor Performance

		COR and technical monitor within one business day of receipt.	technical monitor.	Assessment Reporting System (CPARS).
	Quality	100% of all tasks and products are executed, performed, and completed to the standard described in the requirement; reports demonstrate effective analysis and supported conclusions/ recommendations. Documents returned no more than one time for rework		
TASK 3 – Monthly report	**Timeliness**	98% Monthly report is submitted timely by the scheduled due date; respond to all inquiries from the COR and technical monitor within one business day of receipt.	Review Final Report by COR and technical monitor.	Performance positive or negative will be noted on the Contractor Performance Assessment Reporting System (CPARS).
	Quality	100% of all tasks and products are executed, performed, and completed to the standard described in the requirement; reports demonstrate effective analysis and supported conclusions/ recommendations. Documents returned no more than one time for rework		
TASK 4 – Monthly report	**Timeliness**	98% Monthly report is submitted timely by the scheduled due date; respond to all inquiries from the COR and technical monitor within one business day of receipt.	Review Final Report by COR and technical monitor.	Performance positive or negative will be noted on the Contractor Performance Assessment Reporting System (CPARS).
	Quality	100% of all tasks and products are executed, performed, and completed to the standard described in the requirement; reports demonstrate effective analysis and supported conclusions/ recommendations. Documents returned no more than one time for rework		

TASK 5 – Monthly report	**Timeliness**	98% Monthly report is submitted timely by the scheduled due date; respond to all inquiries from the COR and technical monitor within one business day of receipt.	Review Final Report by COR and technical monitor.	Performance positive or negative will be noted on the Contractor Performance Assessment Reporting System (CPARS).
	Quality	100% of all tasks and products are executed, performed, and completed to the standard described in the requirement; reports demonstrate effective analysis and supported conclusions/ recommendations. Documents returned no more than one time for rework		
TASK 6 – Monthly report	**Timeliness**	98% Monthly report is submitted timely by the scheduled due date; respond to all inquiries from the COR and technical monitor within one business day of receipt.	Review Final Report by COR and technical monitor.	Performance positive or negative will be noted on the Contractor Performance Assessment Reporting System (CPARS).
	Quality	100% of all tasks and products are executed, performed, and completed to the standard described in the requirement; reports demonstrate effective analysis and supported conclusions/ recommendations. Documents returned no more than one time for rework		
TASK 7 – Monthly report	**Timeliness**	98% Monthly report is submitted timely by the scheduled due date; respond to all inquiries from the COR and technical monitor within one business day of receipt.	Review Final Report by COR and technical monitor.	Performance positive or negative will be noted on the Contractor Performance Assessment Reporting System (CPARS).
	Quality	100% of all tasks and products are executed, performed, and completed to the standard described in the requirement; reports demonstrate effective analysis and supported conclusions/ recommendations. Documents returned no more		

		than one time for rework		
FINAL Report	**Timeliness**	98% Final report is submitted by the scheduled due date (that can be no shorter than 3 weeks before the end of contract period); respond to all inquiries from the COR and the technical monitor within one business day of receipt.	Review Final Report by COR and technical monitor.	Performance positive or negative will be noted on the Contractor Performance Assessment Reporting System (CPARS).
	Quality	100% of all tasks and products are reported to the standard described in the requirement; reports demonstrate effective analysis and supported conclusions/ recommendations. Documents returned no more than one time for rework. If final report is not satisfactorily executed during period of performance then contractor will continue work to completion without further charge.		

SECTION 9 – Information Security and Privacy

The below information complies with CDC Security and Privacy compliance requirements for E-Government Act of 2002 (FISMA 2002) and Federal Information Security Modernization Act of 2014 (FISMA 2014)

Security Compliance

- If the contractor will host or create an information system on behalf of the CDC, provide IT services to the CDC, or provide IT products to the CDC, then the contractor shall comply with the applicable IT security references below (Standards 1 - 4).

Standard-1: Procurements Requiring Information Security and/or Physical Access Security

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) employee 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. Protect 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:	[x] Low [ ] Moderate [ ] High
Integrity:	[ ] Low [x] Moderate [ ] High
Availability:	[x] Low [ ] Moderate [ ] High
Overall Risk Level:	[x] Low [ ] Moderate [ ] High

* System contains PII for Non-Sensitive Business Contact Information and by CDC policy determination, Security Categorizations has been changed from Moderate to Low.

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

* System contains PII for Non-Sensitive Business Contact Information and by CDC policy determination, Security Categorizations has been changed from Moderate to Low.

4) **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: [x] Low [ ] Moderate [ ] High

* System contains PII for Non-Sensitive Business Contact Information and by CDC policy determination, Security Categorizations has been changed from Moderate to Low.

5) **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 32 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.*

6) **Protection of Sensitive Information**. For security purposes, information is *or* may be sensitive because it requires security to protect its confidentiality, integrity, and/or availability. The Contractor (and/or any subcontractor) shall protect 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.

7) **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 and *[CDC]* policies. Unauthorized disclosure of information will be subject to the HHS/*[CDC]* 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).

8) **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).* .

9) **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 protect against attacks that attempt to downgrade connections to plain HTTP. For internal-facing websites, the

HTTPS is not required, but it is highly recommended.

10) **Contract Documentation**. The Contractor shall use provided templates, policies, forms and other agency documents to comply with contract deliverables as appropriate.

11) **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 and CDC-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 keyshttp://csrc.nist.gov/publications/. Encryption keys shall be provided to CDC Cybersecurity Program Office (CSPO).

12) **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 CDC 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.

13) **Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA)** – The Contractor shall assist the CDC Senior Official for Privacy (SOP) or designee with conducting a PTA for the information system and/or information handled under this contract in accordance with HHS policy and OMB M-03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.

    a. The Contractor shall assist the CDC 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 CDC SOP that a review is reqnired based on a major change to the system (e.g., new uses of information collected, changes to the way information is shared or disclosed and for what purpose, or when new types of PII are collected that could introduce 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/CDC 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 *CDC Security Awareness Training (SAT), 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 (RBT) ***within***

60 days of assuming their new responsibilities. Thereafter, they shall complete RBT at least ***annually*** in accordance with HHS policy and the *HHS Role-Based Training (RBT) of Personnel with Significant Security Responsibilities Memorandum*.

All HHS employees and contractors with SSR who ***have not*** completed the required training within the mandated timeframes shall have their user accounts disabled until they have met their RBT requirement.
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 *CDC 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

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.

OMB Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information" (03 January 2017) states:

Definition of an Incident:

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.

Definition of a **Breach:**

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.

It further adds:

A breach is not limited to an occurrence where a person other than an authorized user potentially accesses PII by means of a network intrusion, a targeted attack that exploits website vulnerabilities, or an attack executed through an email message or attachment. A breach may also include the loss or theft of physical documents that include PII and portable electronic storage media that store PII, the inadvertent disclosure of PII on a public website, or an oral disclosure of PII to a person who is not authorized to receive that information. It may also include an authorized user accessing PII 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".

Contracts with entities that collect, maintain, use, or operate Federal information or information systems on behalf of CDC shall include the following requirements:

1) The contractor shall cooperate with and exchange information with CDC officials, as deemed necessary by the CDC Breach Response Team, to report and manage a suspected or confirmed breach.

2) All contractors and subcontractors shall properly encrypt PII in accordance with OMB Circular A-130 and other applicable policies, including CDC-specific policies, and comply with HHS-specific policies for protecting PII. To this end, all contractors and subcontractors shall protect 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.

3) All contractors and subcontractors shall participate in regular training on how to identify and report a breach.

4) All contractors and subcontractors shall report a suspected or confirmed breach in any medium as soon as possible and no later than 1 hour of discovery, consistent with applicable CDC IT acquisitions guidance, HHS/CDC and incident management policy, and United States Computer Emergency Readiness Team (US-CERT) notification guidelines. To this end, the Contractor (and/or any subcontractor) shall respond to all alerts/Indicators of Compromise (IOCs) provided by HHS Computer Security Incident Response Center (CSIRC) or CDC Computer Incident Response Team (CSIRT) within 24 hours via email at csirt@cdc.gov or telephone at 866-655-2245, whether the response is positive or negative.

5) All contractors and subcontractors shall be able to determine what Federal information was or could have been accessed and by whom, construct a timeline of user activity, determine methods and techniques used to access Federal information, and identify the initial attack vector.

6) All contractors and subcontractors shall allow for an inspection, investigation, forensic analysis, and any other action necessary to ensure compliance with HHS/CDC Policy and the HHS/CDC Breach Response Plan and to assist with responding to a breach.

7) Cloud service providers shall use guidance provided in the FedRAMP Incident Communications Procedures when deciding when to report directly to US-CERT first or notify CDC first.

8) Identify roles and responsibilities, in accordance with HHS/CDC Breach Response Policy and the HHS/CDC Breach Response Plan. To this end, the Contractor shall NOT notify affected individuals unless and until so instructed by the Contracting Officer or designated representative. If so instructed by the Contracting Officer or representative, all notifications must be pre-approved by the appropriate CDC officials, consistent with HHS/CDC Breach Response Plan, and the Contractor shall then send CDC-approved notifications to affected individuals; and,

9) Acknowledge that CDC will not interpret report of a breach, by itself, as conclusive evidence that the contractor or its subcontractor failed to provide adequate safeguards for PII.

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).

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.*

For additional information, see HSPD-12 policy at: https://www.dhs.gov/homeland-security-presidential-directive-12)

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 by the effective date of this contract. Any revisions to the roster as a result of staffing changes shall be submitted immediately upon 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

1) **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

2) **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.

3) **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*.

4) **Notification.** The Contractor (and/or any subcontractor) shall notify the CO and/or COR and system ISSO before an employee stops working under this contract.

5) **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 *CDC* policies.

6) The Contractor (and/or any subcontractor) shall perform and document the actions identified in the CDC Out-Processing Checklist (http://intranet.cdc.gov/od/hcrmo/pdfs/hr/Out_Processing_Checklist.pdf) when an employee terminates work under this 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 policies and shall not dispose of any records unless authorized by HHS.

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 policies.

Standard-2: Requirements for Procurements Involving Privacy

Appropriate security controls and Rules of Behavior should be incorporated to protect the confidentiality of information, proprietary, sensitive, and Personally Identifiable Information (PII) the Contractor may come in contact with during the performance of this contract.

Standard-3: Procurements Involving Government Information Processed on GOCO or COCO Systems

A. Security Requirements for GOCO and COCO Resources

1) **Federal Policies.** The Contractor (and/or any subcontractor) shall comply with applicable federal directives that include, but are not limited to, the *HHS Information Security and Privacy Policy (IS2P)*, the *CDC Protection of Information Resources* policy; *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 protect 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 prior to any use of the system in a production capacity, i.e., its intended users able to collect, store, process or transmit data to fulfill the system's function. The Contractor shall conduct the SA&A requirements in accordance with *HHS IS2P/ CDC Protection of Information Resources*; the *CDC IT Security Program Implementation Standards;* the *CDC Security Assessment and Authorization (SA&A) Standard Operating Procedure;* and NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (latest revision).

CDC 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 to the C/I/O Information System Security Officer (ISSO) in accordance with the timeline, process and formats proscribed for a Full system authorization in the CDC Security Assessment and Authorization Standard Operating Procedure (CDC SA&A SOP). The following SA&A deliverables are required to complete the SA&A package:

- **Baseline System Information (BSI)** – The Contractor will document a system overview, in accordance with the timeline, process and formats described in the *CDC SA&A SOP*. The BSI will include information concerning: system identification and ownership; system data, information types, impact levels and system categorization; system functional description / general purpose; system authorization boundary and environment; system user descriptions; and system interconnections and dependencies. The Contractor shall update the BSI at least ***annually*** thereafter.

- **Privacy Threshold Analysis / Privacy Impact Analysis** – The Contractor (and/or any subcontractor) shall provide a PTA/PIA (as appropriate), in accordance with the timeline, process and formats described in the *CDC SA&A SOP*, if applicable. Also see the sections of this contract concerning "Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA)" and "Requirements for Procurements Involving Privacy Act Records."

NOTE: If social security numbers (SSN) are expected to be handled by the system, the program and Contractor must include a *SSN Elimination or Usage Approval Request* along with the PTA/PIA. That request will be processed in accordance with the *CSPO Standard for Limiting the Use of Social Security Numbers in CDC Information Systems.*

- **System Security Plan (SSP)** – The SSP must be provided in a digital format supporting copy or export of all content into the HHS/CDC automated SA&A tool. 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 and CDC policies and other guidance. The SSP shall be consistent with and detail the approach to IT security contained in the Contractor's bid or proposal that resulted in the award of this contract. The SSP shall provide an overview of the system environment (including an inventory of all devices and software contained within the system boundary) and security requirements to protect 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.

- **Risk Assessment Report (RAR)** The initial security assessment shall be conducted by the Contractor in conjunction with the program's Information System Security Officer, consistent with NIST SP 800-53A, NIST SP 800-30, and HHS and CDC policies. The assessor will document and submit the assessment results in the RAR, in accordance with the process and formats described in the *CDC SA&A SOP*. 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) for CDC CSPO approval in accordance with the *CDC SA&A SOP*. Thereafter, the Contractor, in coordination with *CDC* shall conduct an assessment of the security controls and update the RAR within 365 days.

  POA&M –The POA&M shall be documented consistent with the HHS Standard for Plan of Action and Milestones and CDC policies. 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 Security Assessment Report (SAR), shall be documented and tracked by the Contractor for mitigation in the POA&M document. Depending on the severity of the risks, CDC 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 and CDC 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 Assessment** – 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; NIST SP 800-63, *Digital Identity Guidelines;* the *CSPO Standard for Electronic Authentication (E-Authentication); and* the *CDC SA&A SOP*.

  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 by specified due date.
- **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 annually. 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 annually. The contractor shall maintain a capability to provide security configuration compliance information for 100% of its IT assets using SCAP-compliant automated tools.
- **Vulnerability Management -** 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 annually.

Critical –	within 15 days
High –	within 30 days
Medium –	within 60 days
Low –	within 350 days

- **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 timeline per CSPO Vulnerability Remediation Framework Standard.
- **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).

1) **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.

2) **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*.

3) **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 information categorized as moderate or high impact as required by OMB Memorandum A-130, *Managing Information as Strategic Resource*, in accordance with the HHS *Standard for Encryption of Computing Devices and Information* and FIPS 140-2.

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) **Change Management.** Once a system is authorized, all changes must be approved by CDC in accordance with NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations;* the *HHS IS2P;* and the timeline, process and formats proscribed in the CDC *CSPO Change Management Standard Operating Procedure*.

5) **Retirement / Decommissioning.** When the CDC program and Contractor determine the system is no longer required, it must be decommissioned in accordance NIST SP 800-88, *Guidelines for Media Sanitization*; the *HHS IS2P;* and the timeline, process and formats proscribed in the CDC *CSPO System Retirement Standard Operating Procedure*.

Standard-4: **Contracts Involving Cloud Services**

HHS FedRAMP Privacy and Security Requirements

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

1) **FedRAMP Compliant ATO**. Comply with FedRAMP Security Assessment and Authorization (SA&A) requirements and ensure the information system/service under this contract has a valid FedRAMP compliant (approved) authority to operate (ATO) in accordance with Federal Information Processing Standard (FIPS) Publication 199 defined security categorization. If a FedRAMP compliant ATO has not been granted, the Contractor shall submit a plan to obtain a FedRAMP compliant ATO.

a. Implement applicable FedRAMP baseline controls commensurate with the agency-defined security categorization and the applicable FedRAMP security control baseline (www.FedRAMP.gov). The *HHS Information Security and Privacy Policy (IS2P)* and *HHS Cloud Computing and Federal Risk and Authorization Management Program (FedRAMP) Guidance* further define the baseline policies as well as roles and responsibilities. The Contractor shall also implement a set of additional controls identified by the agency when applicable.

b. A security control assessment must be conducted by a FedRAMP third-party assessment organization (3PAO) for the initial ATO and annually thereafter or whenever there is a significant change to the system's security posture in accordance with the FedRAMP Continuous Monitoring Plan.

2) **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.

3) **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 CDC to develop and maintain an SLA.

4) **Interconnection Agreements/Memorandum of Agreements.** The Contractor shall establish and maintain Interconnection Agreements and or Memorandum of Agreements/Understanding in accordance with HHS/CDC policies.

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 protect it to the same extent they would the proprietary data and/or company trade secrets and in accordance with HHS/CDC 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 FedRAMP requirements and HHS 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/CDC. 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 contract language herein related to "Requirements for Procurements Involving Privacy Act Records".

1.0- Security Assessment and Authorization (SA&A) Process

1) The Contractor (and/or any subcontractor) shall comply with HHS and FedRAMP 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/CDC security policies and in accordance with the contract language herein related to "Procurements Involving Government Information Processed on GOCO or COCO Systems".

   a. In addition to the FedRAMP compliant ATO, the contractor shall complete and maintain an agency SA&A package to obtain agency ATO prior to system deployment/service implementation in accordance with the contract language herein related to "Procurements Involving Government Information Processed on GOCO or COCO Systems". The agency ATO must be approved by the CDC Authorizing Official (AO) prior to implementation of system and/or service being acquired.

   b. CSP systems must leverage a FedRAMP accredited third-party assessment organization (3PAO).

   c. For all acquired cloud services, the SA&A package must contain documentation in accordance with the contract language herein related to "Procurements Involving Government Information Processed on GOCO or COCO Systems". Following the initial ATO, the Contractor must review and maintain the ATO in accordance with HHS/CDC policies.

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 FedRAMP 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 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 For all system-level weaknesses, the following are specified mitigation timelines from weakness creation date in the POA&M:

    a. **15 days** for critical weaknesses;

    b. **30 days** for high weaknesses;

    c. **60 days** for medium weaknesses; and

    d. **365 days** for low weakness.

    e. HHS will determine the risk rating of vulnerabilities using FedRAMP baselines.

5) **Revocation of a Cloud Service**. HHS/[CDC/OCIO] have 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 and FedRAMP security and privacy requirements and/or there is an incident involving sensitive information, HHS and/or /CDC/ 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.

Reporting and Continuous Monitoring

1) Following the initial ATOs, the Contractor (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 Contractor must provide the following artifacts/deliverables on a ***monthly*** basis:

    a. <u>Vendor/Contractor that owns infrastructure where the system resides:</u>

        i. Perform periodic Authenticated Vulnerability Scans and Application Scans (if applicable) according to CSPO ISCM guidance

        ii. Perform weekly scans (at a minimum) and provide results to C/I/O/ISSO and CSPO ISCM for systems with a FIPS 199 impact level of High, HVA, or if the system contains PII, and ensure scan results are submitted in either CSV or PDF format

        iii. Remediate vulnerabilities in accordance with CSPO Vulnerability Remediation Framework Policy

        iv. Advise the C/I/O/ISSO for any instance when critical/high vulnerabilities cannot be remediated as in accordance with the CSPO Vulnerability Framework Standard

        v. Submit monthly Authenticated Vulnerability scans and Application scans (if applicable) to CDC (business owner) and C/I/O/ISSO

b. Business Stewards (such as System Owner):

i. Confirm Vendor/Contractor is performing Authenticated Vulnerability Scans and Application Scans (if applicable) according to CSPO ISCM guidance

ii. Review monthly Authenticated Vulnerability Scans and Application Scans (if applicable); Develop POA&Ms as needed

iii. Submit monthly Authenticated Vulnerability Scans and Application Scans (if applicable) to CSPO ISCM

iv. Submit written waiver requests to the CISO when systems cannot comply with the provisions of this standard

v. Track remediation/mitigation of security gaps to closure

c. Operating system, database, Web application, and network vulnerability scan results;

d. Updated POA&Ms;

e. Any updated authorization package documentation as required by the annual attestation/assessment/review or as requested by the System Owner or AO; and

f. Any configuration changes to the system and/or system components or CSP's cloud environment, that may impact HHS/CDC'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.

Configuration Baseline

1) The contractor 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/CDC configuration baseline.

2) The 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.

Incident Reporting

1) The Contractor (and/or any subcontractor) shall provide an Incident and Breach Response Plan (IRP) in accordance with HHS CDC, OMB, and US-CERT requirements and obtain approval from the CDC. In addition, the Contractor must follow the incident response and US-CERT reporting guidance contained in the FedRAMP Incident Communications.

2) 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/CDC personnel, or agents acting on behalf of HHS/CDC, 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.

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 protect the confidentiality, integrity, and availability of all government information transported outside of controlled facilities.

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.

Section D - Packaging And Marking

There are no terms and conditions in this section.

Section E - Inspection And Acceptance

E.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):

https://acquisition.gov
(End of Clause)

FAR SOURCE	TITLE AND DATE
52.246-6	Inspection-Time-and-Material and Labor-Hour (May 2001)

Section F - Deliveries Or Performance

F.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):
https://www.acquisition.gov/browse/index/far

(End of Clause)

FAR SOURCE	TITLE AND DATE
52.242-15	Stop-Work Order (Aug 1989)

Section G - Contract Administration Data

G.1 Contract Representative

Contracting Officer (CO) responsible for this contract:
Sarah Turner
Office of Acquisition Services (OAS)
Office of Financial Resources (OFR)
Office of the Chief Operating Officer (OCOO)
Centers for Disease Control and Prevention (CDC)
KWP9@cdc.gov | 404-498-5613

Contracting Officer's Representative (COR) responsible for this contract:
Cate Shockey
DDID/NCEZID/DGMQ
Centers for Disease Control and Prevention (CDC)
404.639.5028, gqw6@cdc.gov
(End of Clause)

G.2 CDCP_G009 Contracting Officer (Jnl 1999)

(a) The Contracting Officer is the only individual who can legally commit the Government to the expenditure of public funds. No person other than the Contracting Officer can make any changes to the terms, conditions, general provisions, or other stipulations of this contract.

(b) No information, other than that which may be contained in an authorized modification to this contract, duly issued by the Contracting Officer, which may be received from any person employed by the United States Government, or otherwise, shall be considered grounds for deviation from any stipulation of this contract.

(End of Clause)

G.3 CDC0_G008 Contracting Officer's Representative (COR) (Jul 2017)

Performance of the work hereunder shall be subject to the technical directions of the designated COR for this contract.

As used herein, technical directions are directions to the Contractor which fill in details, suggests possible lines of inquiry, or otherwise completes tbe general scope of work set forth herein. These technical directions must be within the general scope of work, and may not alter the scope of work or cause changes of such a nature as to justify an adjustment in the stated contract price/cost, or any stated limitation thereof.
In the event that the Contractor believes full implementation of any of these directions may exceed tbe scope of the contract, he or she shall notify the originator of the technical direction and the Contracting Officer, immediately or as soon as possible, in a letter or e-mail separate of any required report(s). No technical direction, nor its fulfillment, shall alter or abrogate the rights and obligations fixed in this contract.

The Government COR is not authorized to change any of the terms and conditions of this contract. Contract changes shall be made only by the Contracting Officer by properly written modification(s) to the contract.

The Government will provide the Contractor with a copy of the COR delegation memorandum upon request.

(End of Clause)

G.4 CDC0_G018 Payment by Electronic Funds Transfer (Feb 2018)

(a) The Government shall use electronic funds transfer to the maximum extent possible when making payments under this contract. FAR 52.232-33, Payment by Electronic Funds Transfer – System for Award Management, in Section I, requires the contractor to designate in writing a financial institution for receipt of electronic funds transfer payments.

(b) In the case that EFT information is not within the System of Award Management, FAR 52.232-34 requires mandatory submission of Contractor's EFT information directly to the office designated in this contract to receive that information (hereafter: "designated office"); see below. The contractor shall submit the EFT information within the form titled "ACH Vendor/Miscellaneous Payment Enrollment Form" to the address indicated below. Note: The form is either attached to this contract (see Section J, List of Attachments) or may be obtained by contacting the Contracting Officer or the CDC Office of Financial Resources at 678-475-4510.

(c) In cases where the contractor has previously provided such information, i.e., pursuant to a prior contract/order, and been enrolled in the program, the form is not required unless the designated financial institution has changed.

(d) The completed form shall be mailed after award, but no later than 14 calendar days before an invoice is submitted, to the following address:
The Centers for Disease Control and Prevention
Office of Financial Resources (OFR)
P.O. Box 15580
Atlanta, GA 30333
Or – Fax copy to: 404-638-5342

(End of Clause)

G.5 CDCA_G001 – Invoice Submission (March 2021)

(a) The Contractor shall submit the original contract invoice/voucher in one of the

following ways: 1) mail, 2) facsimile, 3) email:

Mailing Address:

The Centers for Disease Control and Prevention
Office of Financial Resources (OFR)

P.O. Box
15580 Atlanta,
GA 30333

Fax: 404-638-5324

Email: cpbapinv@cdc.gov

NOTE: Submit only one Invoice in PDF format per attachment.

(b) Subject Line must contain the word "Invoice" Example: Subject: Invoice SAM12345 for Contract 75D30121**********

(c) The content/details of the email must include the below information provided in the body of the email:

- Contract or PO Number:
- Invoice Number:
- Amount:
- Vendor Name:

Only one invoice can be sent to the mailbox with the above relevant details in the body (multiple invoices need to be sent in multiple emails)

(d) The contractor shall submit 2 copies of the invoice to the cognizant contracting office previously identified in this contract. These invoice copies shall be addressed to the attention of the Contracting Officer.

(e) Do not send Links, Zip Files, or .DAT files containing PDF Invoices

(f) The Contractor ☒ is, ☐ is not required to submit a copy of each invoice directly to the Contracting Officer's Representative (COR) concurrently with submission to the Contracting Officer.

(g) In accordance with 5 CFR part 1315 (Prompt Payment), CDC's Office of Financial Resources is the designated billing office for the purpose of determining the payment due date under FAR 32.904.

(h) The Contractor shall include (as a minimum) the following information on each invoice:

(1) Contractor's Name & Address
(2) Contractor's Tax Identification Number (TIN)

(3) Purchase Order/Contract Number and Task Order Number, if Appropriate

(4) Invoice Number
(5) Invoice Date
(6) Contract Line Item Number and Description of Item
(7) Quantity
(8) Unit Price & Extended Amount for each line item
(9) Shipping and Payment Terms
(10) Total Amount of Invoice
(11) Name, title and telephone number of person to be notified in the event of a defective invoice
(12) Payment Address, if different from the information in (c)(1).
(13) DUNS + 4 Number
(14) Electronic funds transfer (EFT) banking info

For the status of invoices, please contact the OFR Service desk at ofrservicedesk@cdc.gov

NOTE: If your invoice has supporting documents, please combine the invoice and supporting documents as one PDF file. Do not submit the invoice and its supporting documents separately.

Section H - Special Contract Requirements

H.1 CDC0_H049 Non-Disclosure Agreement for Contractor and Contractor Employees (Jun 2020)

(a) The contractor and contractor employees shall prepare and submit Non-Disclosure Agreements (NDA) to the Contracting Officer prior to access of government information or the commencement of work at CDC.

(b) The NDAs, at Exhibit I and II, are required in service contracts where contractor's employees will have access to non-public and procurement-sensitive information while performing functions in support of the Government. The NDA also requires contractor's employees properly identify themselves as employees of a contractor when communicating or interacting with CDC employees, employees of other governmental entities, and members of the public (when communication or interaction relates to the contractor's work with the CDC). The Federal Acquisition Regulation (FAR) 37.114 (c), states "All contractor personnel attending meetings, answering Government telephones, and working in other situations where their contractor status is not obvious to third parties are required to identify themselves as such to avoid creating an impression in the minds of members of the public or Congress that they are Government officials, unless, in the judgment of the agency, no harm can come from failing to identify themselves. They must also ensure that all documents or reports produced by contractors are suitably marked as contractor products or that contractor participation is appropriately disclosed."

(c) The contractor shall inform contractor employees of the identification requirements by which they must abide and monitor employee compliance with the identification requirements.

(d) During the contract performance period, the contractor is responsible to ensure that all additional or replacement contractors' employees sign an NDA and it is submitted to the Contracting Officer prior to commencement of their work with the CDC.

(e) Contractor employees in designated positions or functions that have not signed the appropriate NDA shall not have access to any non-public, procurement sensitive information or participate in government meetings where sensitive information may be discussed.

(f) The Contractor shall prepare and maintain a current list of employees working under NDAs and submit to the Contracting Officer upon request during the contract period of performance. The list should at a minimum include: contract number, employee's name, position, date of hire and NDA requirement.

EXHIBIT I
Centers for Disease Control and Prevention (CDC)
Contractor Non-Disclosure Agreement

I. Non-public Information

[Name of contractor] understands that in order to fulfill the responsibilities pursuant to **[contract name and number]** between the Centers for Disease Control and Prevention and **[Name of CDC contractor] dated [date],** employees of **[contractor]** will have access to non-public information, including confidential and privileged information contained in government-owned information technology systems. For purposes of this agreement, confidential information means government information that is not or will not be generally available to the public. Privileged information means information which cannot be disclosed without the prior written consent of the CDC.

In order to properly safeguard non-public information, **[contractor]** agrees to ensure that prior to being granted access to government information or the commencement of work for the CDC, whichever is applicable, all contractor employees will sign a Non-Disclosure Agreement (NDA) provided by the CDC prior to beginning work for the CDC. Contractor agrees to submit to the Contracting Officer the original signed copies of NDAs signed by the contractor's employees in accordance with the instructions provided by the Contracting Officer. Failure to provide signed NDAs in accordance with this agreement and instructions provided by the Contracting Officer could delay or prevent the employee from commencing or continuing work at the CDC until such agreement is signed and returned to the Contracting Officer.

Contractor further agrees that it will not cause or encourage any employee to disclose, publish, divulge, release, or make known in any manner or to any extent, to any individual other than an authorized Government employee any non-public information that the employee may obtain in connection with the performance of the employee's responsibilities to the CDC.

II. Procurement-Sensitive Information

Contractor further agrees that it will not cause or encourage any employee to disclose, publish, divulge, release, or make known in any manner or to any extent, to any individual, other than an authorized Government employee, any procurement-sensitive information gained while in connection with fulfilling the employee's responsibilities at the CDC. For purposes of this agreement, procurement-sensitive information includes, but is not limited to, all information in Statements of Work (SOW), Procurement Requests (PR), and Requests for Proposal (RFP); Responses to RFPs, including proposals, questions from potential offerors; non-public information regarding procurements; all documents, conversations, discussions, data, correspondence, electronic mail (e-mail), presentations, or any other written or verbal communications relating to, concerning, or affecting proposed or pending solicitations or awards; procurement data; contract information plans; strategies; source selection information and documentation; offerors' identities; technical and cost data; the identity of government personnel involved in the solicitation; the schedule of key technical and procurement events in the award determination process; and any other information that may provide an unfair

competitive advantage to a contractor or potential contractor if improperly disclosed to them, or any of their employees.

Contractor understands and agrees that employee access to any procurement-sensitive information may create a conflict of interest which will preclude contractor from becoming a competitor for any acquisition(s) resulting from this information. Therefore, if an employee participates in any discussions relating to procurement-sensitive information, assists in developing any procurement-sensitive information, or otherwise obtains any procurement-sensitive information while performing duties at the CDC, contractor understands and agrees that contractor may be excluded from competing for any acquisition(s) resulting from this information.

III. Identification of Non-Government Employees

Contractor understands that its employees are not agents of the Government. Therefore, unless otherwise directed in writing by the CDC, contractor agrees to assist and monitor employee compliance with the following identification procedures:

A. At the beginning of interactions with CDC employees, employees of other governmental entities, and members of the public (when such communication or interaction relates to the contractor's work with the CDC), contractors' employees will identify themselves as an employee of a contractor.

B. Contractors' employees will include the following disclosures in all written communications, including outgoing electronic mail (e-mail) messages, in connection with contractual duties to the CDC:

Employee's name
Name of contractor
Center or office affiliation
Centers for Disease Control and Prevention

C. At the beginning of telephone conversations or conference calls, contractors' employees will identify themselves as an employee of a contractor.

D. Contractors' employees should not wear any CDC logo on clothing, except for a CDC issued security badge while carrying out work for CDC or on CDC premises. The only other exception is when a CDC management official has granted permission to use the CDC logo.

E. Contractors' employees will program CDC voice mail message to identify themselves as an employee of a contractor.

I understand that federal laws including, 18 U.S.C. 641 and 18 U.S.C. 2071, provide criminal penalties for, among other things, unlawfully removing, destroying or converting to personal use, or use of another, any public records. Contractor acknowledges that contractor has read and fully understands this agreement.

Name of contractor: _____

Signature of Authorized Representative of Contractor:_____

Date:_____

Copies retained by: Contracting Officer and contractor

EXHIBIT II

Centers for Disease Control and Prevention (CDC)
Contractors' Employee Non-Disclosure Agreement

I. Non-Public Information

I understand that in order to fulfill my responsibilities as an employee of **[Name of CDC contractor],** I will have access to non-public information, including confidential and privileged information contained in government-owned information technology systems. For purposes of this agreement, confidential information means government information that is not or will not be generally available to the public. Privileged information means information which cannot be disclosed without the prior written consent of the CDC.

I, **[Name of Employee],** agree to use non-public information only in performance of my responsibilities to the CDC. I agree further that I will not disclose, publish, divulge, release, or make known in any manner or to any extent, to any individual other than an authorized Government employee, any non-public information that I may obtain in connection with the performance of my responsibilities to the CDC.

II. Procurement-Sensitive Information

I further agree that unless I have prior written permission from the CDC, I will not disclose, publish, divulge, release, or make known in any manner or to any extent, to any individual other than an authorized Government employee, any procurement-sensitive information gained in connection with the performance of my responsibilities to the CDC. I specifically agree not to disclose any non-public, procurement-sensitive information to employees of my company or any other organization unless so authorized in writing by the CDC. For purposes of this agreement, procurement-sensitive information includes, but is not limited to, all information in Statements of Work (SOW), Procurement Requests (PR), and Requests for Proposal (RFP); Responses to RFPs, including proposals, questions from potential offerors; non-public information regarding procurements; all documents, conversations, discussions, data, correspondence, electronic mail (e-mail), presentations, or any other written or verbal communications relating to, concerning, or affecting proposed or pending solicitations or awards; procurement data; contract information plans; strategies; source selection information and documentation; offerors' identities; technical and cost data; the identity of government personnel involved in the acquisition; the schedule of key technical and procurement events in the award determination process; and any other information that may provide an unfair competitive advantage to a contractor or potential contractor if improperly disclosed to them, or any of their employees.

I understand and agree that my access to any procurement-sensitive information may create a conflict of interest which will preclude me, my current employer, or a future employer from becoming a competitor for any resulting government acquisition derived from this information. Therefore, if I participate in any discussions relating to procurement-sensitive information, assist in developing any procurement-sensitive information, or otherwise obtain any procurement-sensitive information while performing my duties at the CDC, I understand and agree that I, my

current employer, and any future employer(s) may be excluded from competing for any resulting acquisitions.

III. Special Non-Disclosure Agreement for Contractors with Access to CDC Grants Management and Procurement-Related Information Technology Systems

In addition to complying with the non-disclosure requirements and safeguards stated above, I understand that my authorization to use CDC's grants management and procurement systems is strictly limited to the access and functions necessary for the performance of my responsibilities to the CDC and which have been approved in advance by the CDC. I understand that I am not authorized to enter procurement requests for any requirements pertaining to contracts or subcontracts held by me or my employer.

IV. Identification as a Non-Government Employee

I understand that as an employee of a government contractor, I represent an independent organization and I am not an agent of the Government. Therefore, I agree that unless I have prior written authorization from the CDC, I will, at the beginning of interactions with CDC employees, employees of other governmental entities, members of the public (when such communication or interaction relates to the contractor's work with the CDC), identify myself as an employee of a contractor. I further agree to use the following identification procedures in connection with my work at the CDC:

A. I will include the following disclosures in all written communications, including outgoing electronic mail (e-mail) messages:

Employee's name
Name of contractor
Center or office affiliation
Centers for Disease Control and Prevention

B. I will identify myself as an employee of a contractor at the beginning of telephone conversations or conference calls;
C. I will not wear any CDC logo on clothing, except for a CDC issued security badge while carrying out work for CDC or on CDC premises; the only other exception is when a CDC management official has granted permission to use the CDC logo.
D. I will program my CDC voice mail message to identify myself as a contractors' employee.

I understand that federal laws including, 18 U.S.C. 641 and 18 U.S.C. 2071, provide criminal penalties for, among other things, unlawfully removing, destroying or converting to personal use, or use of another, any public records. I acknowledge that I have read and fully understand this agreement.

Name of contractor: _____

Name of Employee:_____

Signature of Employee:_____

Date:_____

Copies retained by: Contracting Officer, contractor, and Contractor Employee

H.2 CDC0_H022 Smoke Free Working Environment (May 2009)

In compliance with Department of Health and Human Services (DHHS) regulations, all contractor personnel performing work within CDC/ATSDR facilities shall observe the CDC/ATSDR smoke-free working environment policy at all times. This policy prohibits smoking in all CDC/ATSDR buildings and in front of buildings which are open to the public. This policy is also applicable to contractor personnel who do not work full-time within CDC/ATSDR facilities, but are attending meetings within CDC/ATSDR facilities.

(End of Clause)

H.3 CDC37.0001 Non-Personal Services (Jun 2020)

(a) Personal services shall not be performed under this contract. Although the Government may provide sporadic or occasional instructions within the scope of the contract, the Contractor is responsible for control and supervision of its employees. If the Contractor (including its employees) believes any Government action or communication has been given that would create a personal services relationship between the Government and any Contractor employee, the Contractor shall promptly notify the Contracting Officer of this communication or action.

(b) The contractor shall comply with, and ensure their employees and subcontractors comply with, CDC Policy titled "Contractor Identification and Safeguarding of Non-Public Information". No Contractor employee shall hold him or herself out to be 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. In all communications with third parties in connection with this contract, Contractor employees shall identify themselves as Contractor employees and specify the name of the company for which they work. The contractor is limited to performing the services identified in the contract statement of work and shall not interpret any communication with anyone as a permissible change in contract scope or as authorization to perform work not described in the contract. All contract changes will be incorporated by a modification signed by the Contracting Officer.

(c) The Contractor shall ensure that all of its employees and subcontractor employees working on this contract are informed of the terms and conditions herein. The Contractor agrees that this is a non-personal services contract; and that for all the purposes of the contract, the Contractor is not, nor shall it hold itself out to be an agent or partner of, or joint venture with, the Government. The Contractor shall notify its employees that they shall neither supervise nor accept supervision

from Government employees. The substance of the terms herein shall be included in all subcontracts at any tier.

(d) The terms and conditions above do not limit the Government's rights under other terms of the contract, including those related to the Government's right to inspect and accept or reject the services performed under this contract.

H.4 - CDCA_H040 Government Property (July 2017)

(a) Government-Furnished Property (GFP). In accordance with the terms of FAR 52.245-1, Government Property, the Government reserves the right to supply the Contractor, as Government-furnished property, any additional supplies, equipment, and materials determined by the Contracting Officer to be necessary and in the best interest of the Government.

(b) Contractor-Acquired Property (CAP). The Contractor must receive written consent from the Contracting Officer prior to purchase of any CAP not expressly identified in the contract, and as defined in FAR 52.245-1.

(c) Accountable and Sensitive Government Property. The Government will provide property labels and other identification for contractor-acquired Government property that is considered Accountable as defined in the HHS Logistics Management Manual (LMM) https://intranet.hhs.gov/abouthhs/manuals/lmm/index.html or considered Sensitive as defined in CDC's Sensitive Items List (http://intranet.cdc.gov/ofr/documents/contracts/Authorized-Prohibited-List.pdf)

(d) The contractor shall be responsible for the control and accountable record keeping of any Government property used in the performance of this contract predominately outside the confines of a Government controlled workspace in accordance with the HHS Contracting Guide found on the OSSAM Government Property and Contractors Property intranet page. (http://intranet.cdc.gov/ossam/property-shipping-receiving/property-management/government-property-contractors/index.html)

(e) The Chief of the Office of Safety, Security and Asset Management (OSSAM), Asset Management Services Office, Centers for Disease Control and Prevention (CDC), is hereby designated as the Property Administrator for this contract. The Contractor shall identify each item of equipment furnished by the Government to the Contractor or acquired by the Contractor using contract funds, with a suitable decal, tag, or other marking, as prescribed by the Property Administrator, and shall follow the guidance set forth in the HHS Contracting Guide.

(End of Clause)

H.5 CDCA_H037 Observance of Legal Holidays and Administrative Leave (Government Facilities Performance) (Jul 2021)

(a) Holidays

Government personnel observe the following listed days as holidays:

Washington's Birthday
Memorial Day
Juneteenth
Independence Day
Labor Day
Veterans' Day
Thanksgiving Day
Christmas Day
New Year's Day
Columbus Day
Martin Luther King Day

Any other day designated by Federal Statute
Any other day designated by Executive Order
Any other day designated by Presidential proclamation

For purposes of contract performance, the Contractor shall observe the above holidays on the date observed by the Government. Observance of such days shall not be cause for an additional period of performance or entitlement to compensation except as otherwise set forth in the contract. No form of holiday or other premium compensation will be reimbursed; however this does not preclude reimbursement for overtime work authorized in writing by the Contracting Officer.

(b) Unscheduled Facility Closures

In the event Government facilities are closed due to inclement weather, potentially hazardous or unsafe conditions, or other special circumstances, contractor personnel assigned to work within those facilities are automatically dismissed. Notwithstanding the terms herein, the contractor shall comply with any specific contract terms that require a level of ongoing support for critical operations during times of facility closure. The contractor may also continue to provide support under a scheduled telework arrangement in accordance with the terms of the contract if the contract expressly authorizes telework in writing.

(c) Cost Impact

Accounting for costs associated with an unscheduled facility closure is unique to each contract and depends upon a number of factors such as:

i) Contract type, e.g. Fixed Price, Time and Materials, or Cost Reimbursement.
ii) Contractor's established management and accounting practices for unproductive time.
iii) The inclusion and applicability of other contract terms & conditions.
iv) The ability of the contractor to mitigate costs by reassigning employees to work on other contracts, to work from a different facility, or to work remotely from home in accordance with contract telework provisions.

H.6 Telework by Contractor (Feb 2015)

Telework is the movement of contract performance from a CDC facility to a teleworker's residence or alternate work site. The Contractor's organizational decision to participate in telework is voluntary, and telework shall not increase the contract price. After contract award, telework arrangements shall be mutually agreed to in advance by the Contractor, the Contracting Officer, and the Project Officer. The Contractor shall submit written telework requests to the Contracting Officer in accordance with instructions provided by the Contracting Officer. The Contractor shall ensure the continuity of performance by Teleworkers and the monitoring of Teleworkers' time. CDC staff do not supervise contractor employees and do not approve or monitor contractor employees' telework. Only the Contracting Officer has authority to approve telework arrangements on behalf of CDC.

Teleworkers shall use Government-Furnished Equipment (GFE) that has been properly configured for security by CDC's Information Technology Services Office (ITSO). The Government's inability to provide GFE for telework shall preclude the use of telework but shall not constitute an excusable delay. The Government shall provide maintenance and technical support for GFE used by Teleworkers. A Teleworker's use of GFE and government information shall he for contractual performance only, and shall be protected from unauthorized access, disclosure, sharing, transmission, or loss. Teleworkers shall comply with CDC Policy No. CDCGA- 2005-02, "Use of CDC Information Technology Resources" (see http://aops-masiis.cdc.gov/Policy/Doc/policy90.pdf).

All GFE used for telework shall be removed from and returned to CDC facilities in accordance with CDC Policy CDC-MM-2005-01 "Controls for Government Property and Guidance on Removing Government Property from CDC Facilities" (see http:// aops-mas-iis.od.cdc.gov/Policy/Doc/policy480.htm). Prior to removing GFE from CDC facilities, Teleworkers shall obtain written approval from the CDC Property Custodian. Teleworkers shall return all GFE to the CDC Property Custodian when he/she separates from the Contract or ceases to telework.

Teleworkers shall exercise due care in transporting and storing non-public information, to ensure it is safeguarded. Controlled unclassified information – formerly called sensitive but unclassified (SBU) information under CDC Policy No. CDC-IS-2005-02, "Sensitive by Unclassified Information" (see http://aops-mas-iis.cdc.gov/Policy/Doc/policy464.htm) - including personally identifiable information (PII) and Privacy Act information shall be transported and stored only in encrypted form. Nonpublic government information shall not be stored on personally-owned equipment, devices, or storage media. Teleworkers shall comply with additional information security requirements established by CDC's Office of the Chief Information Security Officer (see http://intranet.cdc.gov/ociso/). Teleworkers shall apply approved safeguards to protect government equipment, records, and non-public information from unauthorized access, disclosure, sharing, transmission, or damage, and shall comply with Privacy Act requirements (Privacy Act of 1974, P.L. 93-579, 5 USC 552a). Violation may result in adverse action, fines, and/or criminal prosecution.

For purposes of accelerated implementation of telework, the Contracting Officer may immediately elect to commence teleworking upon concurrence from the Project Officer and Contractor, with submission of the Contractor's supporting telework request and formal contract modification to follow within 30 calendar days. If the Contracting Officer and Project Officer determine that telework has adversely impacted contract performance, the Contracting Officer may immediately suspend telework arrangements upon written notification to the Contractor

(End of clause)

H.8 CDCA_H042 Records Management Obligations (Jun 2020)

A. *Applicability*

The following applies to all Contractors whose employees create, work with, or otherwise handle Federal records, as defined in Section B, regardless of the medium in which the record exists.

B. *Definitions*

"Federal record" as defined in 44 U.S.C. § 3301, includes all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them.

The term Federal record:

1. includes Centers for Disease Control and Prevention (CDC) records.
2. does not include personal materials.
3. applies to records created, received, or maintained by Contractors pursuant to their CDC contract.
4. may include deliverables and documentation associated with deliverables.

C. *Requirements*

1. Contractor shall comply with all applicable records management laws and regulations, as well as National Archives and Records Administration (NARA) records policies, including but not limited to the Federal Records Act (44 U.S.C. chs. 21, 29, 31, 33), NARA regulations at 36 CFR Chapter XII Subchapter B, and those policies associated with the safeguarding of records covered by the Privacy Act of 1974 (5 U.S.C. 552a). These policies include the preservation of all records, regardless of form or characteristics, mode of transmission, or state of completion.
2. In accordance with 36 CFR 1222.32, all data created for Government use and delivered to, or falling under the legal control of, the Government are Federal records subject to the provisions of 44 U.S.C. chapters 21, 29, 31, and 33, the Freedom of Information Act (FOIA) (5 U.S.C. 552), as amended, and the Privacy Act of 1974 (5 U.S.C. 552a), as

amended and must be managed and scheduled for disposition only as permitted by statute or regulation.

3. In accordance with 36 CFR 1222.32, Contractor shall maintain all records created for Government use or created in the course of performing the contract and/or delivered to, or under the legal control of the Government and must be managed in accordance with Federal law. Electronic records and associated metadata must be accompanied by sufficient technical documentation to permit understanding and use of the records and data.
4. CDC and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Records may not be removed from the legal custody of CDC or destroyed except for in accordance with the provisions of the agency records schedules and with the written concurrence of the Head of the Contracting Activity. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. In the event of any unlawful or accidental removal, defacing, alteration, or destruction of records, Contractor must report to the Contracting Officer and the Contracting Officer's Representative. The agency must report promptly to NARA in accordance with 36 CFR 1230.
5. The Contractor shall immediately notify the appropriate Contracting Officer upon discovery of any inadvertent or unauthorized disclosures of information, data, documentary materials, records or equipment. Disclosure of non-public information is limited to authorized personnel with a need-to-know as described in the contract. The Contractor shall ensure that the appropriate personnel, administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, documentary material, records and/or equipment is properly protected. The Contractor shall not remove material from Government facilities or systems, or facilities or systems operated or maintained on the Government's behalf, without the express written permission of the Head of the Contracting Activity. When information, data, documentary material, records and/or equipment is no longer required, it shall be returned to CDC control or the Contractor must hold it until otherwise directed. Items returned to the Government shall be hand carried, mailed, emailed, or securely electronically transmitted to the Contracting Officer or address prescribed in the contract. Destruction of records is EXPRESSLY PROHIBITED unless in accordance with Paragraph (4).
6. The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (sub-contractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under, or relating to, contracts. The Contractor (and any sub-contractor) is required to abide by Government and CDC guidance for protecting sensitive, proprietary information, classified, and controlled unclassified information.
7. The Contractor shall only use Government IT equipment for purposes specifically tied to or authorized by the contract and in accordance with CDC policy.

8. The Contractor shall not create or maintain any records containing any non-public CDC information that are not specifically tied to or authorized by the contract.
9. The Contractor shall not retain, use, sell, or disseminate copies of any deliverable that contains information covered by the Privacy Act of 1974 or that which is generally protected from public disclosure by an exemption to the Freedom of Information Act.
10. Training. All Contractor employees assigned to this contract who create, work with, or otherwise handle records are required to take CDC-provided records management training. The Contractor is responsible for confirming training has been completed according to agency policies, including initial training and any annual or refresher training.

D. *Flowdown of requirements to subcontractors*

1. The Contractor shall incorporate the entire substance of the terms and conditions herein, including this paragraph, in all subcontracts under this contract, and must require written subcontractor acknowledgment of same.
2. Violation by a subcontractor of any provision set forth herein will be attributed to the Contractor.

Section I - Contract Clauses

Section I-1 - Clauses Incorporated By Reference

I.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):

https://acquisition.gov
(End of Clause)

FAR SOURCE	TITLE AND DATE
52.202-1	Definitions (June 2020)
52.203-3	Gratuities (Apr 1984)
52.203-5	Covenant against Contingent Fees (May 2014)
52.203-6	Restrictions on Subcontractor Sales to the Government (June 2020)
52.203-7	Anti-Kickback Procedures (June 2020)
52.203-8	Cancellation, Rescission, and Recovery of Funds for Illegal or Improper Activity (May 2014)
52.203-10	Price or Fee Adjustment for Illegal or Improper Activity (May 2014)
52.203-12	Limitation on Payments to Influence Certain Federal Transactions (June 2020)
52.203-13	Contractor Code of Business Ethics and Conduct (June 2020)
52.203-17	Contractor Employee Whistleblower Rights and Requirement To Inform Employees of Whistleblower Rights (June 2020)
52.203-19	Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017)
52.204-4	Printed or Copied Double-Sided on Recycled Paper (May 2011)
52.204-9	Personal Identity Verification of Contractor Personnel (Jan 2011)
52.204-10	Reporting Executive Compensation and First-Tier Subcontract Awards (Jun 2020)
52.204-13	System for Award Management Maintenance (Oct 2018)
52.204-14	Service Contract Reporting Requirements (Oct 2016)
52.204-18	Commercial and Governemnt Entity Code Maintenance (Aug 2020)
52.204-19	Incorporation by Reference of Representations and Certifications (Dec 2014)
52.204-23	Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018)
52.204-25	Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (AUG 2020)
52.209-6	Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment (Jun 2020)
52.209-9	Updates of Publicly Available Information Regarding Responsibility Matters (Oct 2018)
52.209-10	Prohibition on Contracting with Inverted Domestic Corporations. (Nov 2015)
52.215-2	Audit and Records -- Negotiation (Jun 2020)

52.215-8	Order of Precedence - Uniform Contract Format (Oct 1997)
52.215-10	Price Reduction for Defective Certified Cost or Pricing Data (Aug 2011)
52.215-11	Price Reduction for Defective Certified Cost or Pricing Data - Modifications (Jun 2020
52.215-12	Subcontractor Certified Cost or Pricing Data (Jun 2020)
52.215-13	Subcontractor Certified Cost or Pricing Data - Modifications (Jun 2020)
52.215-15	Pension Adjustments and Asset Reversions (Oct 2010)
52.215-17	Waiver of Facilities Capital Cost of Money (Oct 1997)
52.215-18	Reversion or Adjustment of Plans for Postretirement Benefits (PRB) Other Than Pensions. (Jul 2005)
52.215-19	Notification of Ownership Changes (Oct 1997)
52.215-21	Requirements for Certified Cost or Pricing Data and Data Other Than Certified Cost or Pricing Data - Modifications (Jun 2020)
52.222-3	Convict Labor (Jun 2003)
52.222-4	Contract Work Hours and Safety Standards Act - Overtime Compensation (May 2018)
52.222-21	Prohibition of Segregated Facilities (Apr 2015)
52.222-26	Equal Opportunity (Sep 2016)
52.222-35	Equal Opportunity for Veterans (Jun 2020)
52.222-36	Equal Opportunity for Workers with Disabilities (Jun 2020)
52.222-37	Employment Reports on Veterans (Jun 2020)
52.222-40	Notification of Employee Rights Under the National Labor Relations Act (Dec 2010)
52.222-50	Combating Trafficking in Persons (Oct 2020)
52.222-54	Employment Eligibility Verification (Oct 2015)
52.223-5	Pollution Prevention and Right-to-Know Information (May 2011)
52.223-6	Drug-Free Workplace (May 2001)
52.223-10	Waste Reduction Program (May 2011)
52.223-18	Encouraging Contractor Policies to Ban Text Messaging While Driving (Jun 2020)
52.224-1	Privacy Act Notification (Apr 1984)
52.224-2	Privacy Act (Apr 1984)
52.225-13	Restrictions on Certain Foreign Purchases (Feb 2021)
52.226-1	Utilization of Indian Organizations and Indian-Owned Economic Enterprises (Jun 2000)
52.227-1	Authorization and Consent (Jun 2020)
52.227-2	Notice and Assistance Regarding Patent and Copyright Infringement (Jun 2020)
52.227-3	Patent Indemnity (Apr 1984)
52.227-14	Rights in Data – General (May 2014)
52.232-7	Payments under Time-and-Materials and Labor-Hour Contracts (Aug 2012)
52.232-9	Limitation on Withholding of Payments (Apr 1984)
52.232-11	Extras (Apr 1984)
52.232-17	Interest (May 2014)
52.232-23	Assignment of Claims (May 2014)
52.232-25	Prompt Payment (Jan 2017)
52.232.33	Payment by Electronic Funds Transfer-- System for Award Management (Oct 2018

52.232-39	Unenforceability of Unauthorized Obligations (Jun 2013)
52.232-40	Providing Accelerated Payments to Small Business Subcontractors (Dec 2013)
52.233-1	Disputes (May 2014)
52.233-3	Protest after Award (Aug. 1996)
52.233-4	Applicable Law for Breach of Contract Claim (Oct 2004)
52.237-2	Protection of Government Buildings, Equipment, and Vegetation (Apr 1984)
52.237-3	Continuity of Services (Jan 1991)
52.237-7	Indemnification and Medical Liability Insurance (Jan 1997)
52.239-1	Privacy or Security Safeguards (Aug 1996)
52.242-13	Bankruptcy (Jul 1995)
53.243-3	Changes - Time-and-Materials or Labor-Hours (Sept 2000)
52.243-7	Notification of Changes (Jan 2017)
52.244-2	Subcontracts (Jun 2020)
52.244-5	Competition in Subcontracting (Dec 1996)
52.244-6	Subcontracts for Commercial Items (Nov 2020)
52.245-1	Government Property (Jan 2017)
52.245-9	Use and Charges (Apr 2012)
52.246-25	Limitation of Liability - Services (Feb 1997)
52.248-1	Value Engineering (Jun 2020)
52.249-6	Termination (Cost-Reimbursement) (May 2004), Alternate IV (May 2004)
52.249-14	Excusable Delays (Apr 1984)
HHSAR SOURCE	**TITLE AND DATE**
352.203-70	Anti-Lobbying (December 18, 2015)
352.208-70	Printing and Duplication (December 18, 2015)
352.222-70	Contractor Cooperations in Equal Employment Opportunity Investigations (December 18, 2015)
352.224-70	Privacy Act (December 18, 2015)
352.224-71	Confidential Information (December 18, 2015)
352.231-70	Salary Rate Limitation (December 18, 2015)
352.233-71	Litigation and Claims (December 18, 2015)
352.237-75	Key Personnel (December 18, 2015)

Section I-2 - Clauses Incorporated In Full Text

I.5 CDC42.0002 Evaluation of Contractor Performance Utilizing CPARS (Apr 2015)

In accordance with FAR 42.15, the Centers for Disease Control and Prevention (CDC) will review and evaluate contract performance. FAR 42.1502 and 42.1503 requires agencies to prepare evaluations of contractor performance and submit them to the Past Performance Information Retrieval System (PPIRS). The CDC utilizes the Department of Defense (DOD) web-based Contractor Performance Assessment Reporting System (CPARS) to prepare and report these contractor performance evaluations. All information contained in these assessments may be used by the Government, within the limitations of FAR 42.15, for future source selections in accordance with FAR 15.304 where past performance is an evaluation factor.

The CPARS system requires a contractor representative to be assigned so that the contractor has appropriate input into the performance evaluation process. The CPARS contractor representative will be given access to CPARS and will be given the opportunity to concur or not-concur with performance evaluations before the evaluations are complete. The CPARS contractor representative will also have the opportunity to add comments to performance evaluations.

The assessment is not subject to the Disputes clause of the contract, nor is it subject to appeal beyond the review and comment procedures described in the guides on the CPARS website. Refer to: www.cpars.gov for details and additional information related to CPARS, CPARS user access, how contract performance assessments are conducted, and how Contractors participate. Access and training for all persons responsible for the preparation and review of performance assessments is also available at the CPARS website.

The contractor must provide the CDC contracting office with the name, e-mail address, and phone number of their designated CPARS representative who will be responsible for logging into CPARS and reviewing and commenting on performance evaluations. The contractor must maintain a current representative to serve as the contractor representative in CPARS. It is the contractor's responsibility to notify the CDC contracting office, in writing (letter or email), when their CPARS representative information needs to be changed or updated. Failure to maintain current CPARS contractor representative information will result in the loss of an opportunity to review and comment on performance evaluations.

[End of Clause]

I.6 HHSAR 352.239-74 Electronic and Information Technology Accessibility. (December 18, 2015)

(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) supplies and services developed, acquired, or maintained under this contract or order must comply with the "Architectural and Transportation Barriers Compliance Board Electronic and Information Technology (EIT) Accessibility Standards" 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.hhs.gov/web/508. The complete text of

Section 508 Final Provisions can be accessed at http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards.

(b) The Section 508 accessibility standards applicable to this contract or order are identified in the Statement of Work or Specification or Performance Work Statement. The contractor must provide any necessary updates to the submitted HHS Product Assessment Template(s) at the end of each contract or order exceeding the simplified acquisition threshold (see FAR 2.101) when the contract or order duration is one year or less. If it is determined by the Government that EIT supplies and services provided by the Contractor do not conform to the described accessibility standards in the contract, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(c) The Section 508 accessibility standards applicable to this contract are: 1194

205 WCAG 2.0 Level A & AA Success Criteria
302 Functional Performance Criteria
502 Inoperability with Assistive Technology
504 Authoring Tools
602 Support Documentation
603 Support Services

(d) In the event of a modification(s) to this contract or order, which adds new EIT supplies or services or revises the type of, or specifications for, supplies or services, the Contracting Officer may require that the contractor submit a completed HHS Section 508 Product Assessment Template and any other additional information necessary to assist the Government in determining that the EIT supplies or services conform to 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 website: (http://www.hhs.gov/web/508). If it is determined by the Government that EIT supplies and services provided by the Contractor do not conform to the described accessibility standards in the contract, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(e) If this is an Indefinite Delivery contract, a Blanket Purchase Agreement or a Basic Ordering Agreement, the task/delivery order requests that include EIT supplies or services will define the specifications and accessibility standards for the order. In those cases, the Contractor may be required to provide a completed HHS Section 508 Product Assessment Template and any other additional information necessary to assist the Government in determining that the EIT supplies or services conform to Section 508 accessibility standards. Instructions for documenting accessibility via the HHS Section 508 Product Assessment Template may be found at http://www.hhs.gov/web/508. If it is determined by the Government that EIT supplies and services provided by the Contractor do not conform to the described accessibility standards in the provided documentation, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(End of clause)

Section C - Performance Work Statement

NCIRD Web Services and Digital Media Communications

C1 BACKGROUND: The National Center for Immunization and Respiratory Diseases (NCIRD) is a critical component within CDC, providing leadership in the prevention of disease, disability, and death through immunization and by control of respiratory and related diseases. NCIRD works to effectively balance our efforts to accommodate the specific needs of all populations at risk of vaccine preventable diseases from children to older adults. It is imperative that NCIRD use digital media to communicate, disseminate, educate and engage on a variety of health topics to its audiences. Digital media tools & channels used by NCIRD include, but are not limited to Web sites, social media, Application Programming Interfaces (APIs), Web applications and mobile apps.

C2 PURPOSE: The objective of this task order is to support CDC NCIRD digital media communication activities by providing NCIRD with support and expertise across all key areas of web and digital media management. This work ensures that NCIRD's activities:

- Are effectively and appropriately managed
- Use appropriate technology
- Are usable and meet audience needs
- Provide users with high-quality and accurate content
- Provide engagement opportunities
- Are searchable, findable, and allow for re-use of content
- Comply with federal, HHS, and CDC policies, standards and best practices
- Are innovative and creative

The specific websites, projects, or tools supported under this project scope may vary during the life of this contract. This contract may be modified to increase or decrease the number of websites, projects or tools supported.

C3 SCOPE: The Government requires high level, professional support capable of bringing expertise and extensive communications experience to elevate the caliber of NCIRD programs.

The contractor shall meet the following criteria in order to effectively complete the tasks outlined in the below description of work.

1. Possess a thorough understanding of the current state, strategic vision and future plans of NCIRD and its programs.
2. Ensure that information products produced and reviewed are of a high standard and error free for electronic and print publication by NCIRD for submission to CDC and external parties, publishers or for posting on CDC's Internet or intranet sites.
3. Ensure that information products are accessible to persons with disabilities (508 compliant) and suitable for electronic and print publication by NCIRD for submission to CDC and external parties, publishers or for posting on CDC's internet,intranet sites and social media platforms.
4. Maintain knowledge of and conform with copyright regulations, publication disclaimers, authorship requirements, conflict-of-interest concerns, use of contractor and partner logos, and CDC communication and identity policies.
5. Conform to writing, editing, and publishing requirements for federal agencies in general and CDC and NCIRD in particular.

As an independent organization, and not as an agent of the government, the Contractor will furnish all necessary personnel to provide NCIRD with Web Services and Digital Media Communications services within the general work parameters set forth in the following tasks:

TASK 1: PROJECT MANAGEMENT: Program Manager(s) will coordinate and track tasks across the team(s) in order to keep processes moving and on schedule, troubleshoot to resolve issues and bottlenecks and monitor, track and report project deliverables and milestones; track and report on web requests and projects using a dashboard that is updated in real time, with a summary provided monthly; plan, implement, evaluate and document program activities using qualitative and quantitative methods and strategies; gather data and coordinate with COR /Technical Monitor to support development of program guidelines, goals, plans, and strategies and respond to inquiries as needed; and collect and assemble data related to the evaluation of digital campaigns or other activities /strategies.

1.1 Kickoff Meeting: A kickoff meeting shall be held no later than **10 work days** after the initial award is made to discuss the contractors workplan and timelines as well as clarify roles and responsibilities.

1.2 Work Plan: The contractor shall provide a written work plan for COR review and acceptance no later than **10 work days** following the kickoff meeting. The work plan will provide clarification or updates specific to each task as discussed in the kickoff meeting, description of reports and activities to be provided by the contractor during the course of the project, and identification of key staff responsible for these tasks. The workplan will capture the final schedule of key deadlines and deliverable dates.

1.3 Monthly Reports: The workplan will be updated **monthly** and provided to the CDC Technical Monitor and COR no later than the last business day of each month. This report is considered a substantial deliverable and will be used as a tracking tool for success of this project, and documentation of effort/services as invoiced in the matching monthly invoice.

TASK 2: WEBSITE SUPPORT SERVICES: Support for this task will focus on management of NCIRD web properties including internet and intranet sites. The specific websites, projects, or tools supported under this project may vary during the life of this contract. The current NCIRD web portfolio consists of **45+** web sites, **3,500+** HTML web pages and **2,500+** web files (see Appendix A for full list of websites). The number of websites and types of requests will vary and depends upon agency needs each year, especially in the event of a public health emergency (see Optional TASK 5).

2.1 Web Maintenance and Design. The contractor shall provide day-to-day maintenance of NCIRD Websites using CDC's standard Web Content Management System (WCMS) (See Appendix A for QA Site QA Review Process and Appendix B for WCMS Checklist). The contractor will support development of and update webpages using Web software applications, techniques, and tools using Web-based technologies such as Extensible Markup Language (XML), Hyper Text Markup Language (HTML)/HTML5, JavaScript (JS)/jQuery, Cascading Style Sheets (CSS)/CSS3, Photoshop, and other design-related applications. The contractor will support design efforts to enhance look and feel of NCIRD's web sites and design Website(s) to support user needs as well as organization communication strategies and goals. This will include ensurance that each page displays correctly in all view ports and is cross-browser and device compatible to support responsive web design. All web pages must comply with all federal, HHS and CDC standards. The contractor shall use CDC approved Web tools to check and validate the page code, checking multiple viewpoints, metrics reports, and ensure the quality of our Web sites using the Site QA Review Process (See in Appendix A for Site QA Review Process). Managed Web content should be appropriately marked up, tagged/coded and maintained for search engine optimization and Social Media sharing, using CDC's APIs and adhering to Section 508/WCAG compliance. The contractor will also provide Web site monitoring to include: digital first, quality assurance, accessibility, SEO, response, and compliance with polices and standards.

2.2 Web Management Tools: The contractor shall provide support in the maintenance of internal web management tools and forms used to manage web requests, projects, and reporting tools within SharePoint. The contractor will use Web Request Form tocapture data on key performance metrics including numbers of web requests, level of complexity of work, and

estimated resources expended. The contractor will also use data to create dashboards that are updated monthly that document updates to CDC's websites and the level of effort to support those efforts.

2.3 Spanish Language Web Support: The contractor shall provide technical oversight over the Spanish language pages and have expertise in Spanish language, ideally from a cultural expert or native speaker. Support for this task will include recommending existing NCIRD English webpages for translation and coordinate with CDC's multilingual services or other translation product providers to get pages translated and provide quality assurance for all translations. The contractor may also provide recommendation of culturally appropriate images and visuals. Refer to APPENDIX A.

2.4 E-mail Communication Tools: The contractor shall provide technical oversight for e-mail communication tools that provide e-mail messages and e-newsletter through communication platforms, such as Adobe Campaign, or whichever product or service is in use by CDC. The contractor will support NCIRD in developing and maintaining a robust list of organizational e-mails of partners, awardees, NGOs and others key for distribution of e-newsletters and other web-based communications. The contractor will validate and update quarterly and provide training and documentation in use of the tool(s) as needed.

2.5 Programming: The contractor shall provide operations and maintenance (O&M) programming support for maintenance of NCIRD's web applications and 3 mobile apps s (*in accordance with EPLC Policy*) (See current list in Appendix A). This will include ensuring the applications are revised when operating systems change, technical updates are needed, and support updates in content and functionality. It is anticipated this work would consist primarily of maintenance, functionality improvements, and content updates to the existing applications. That contractor shall provide accurate coding in extremely tight timeframe, testing using real time data, and 508 testing for specific applications within a constantly evolving environment. Senior level skills of CDC's current programming in ASP.NET, CDC's current SQL server environment, JavaScript, and writing complex scripts are required for web applications. Require senior level programming skills in Cordova.js, the latest version of jQuery, jQuery Mobile, swift (XCode), and Java (Android Studio) for mobile apps.

2.6 User Experience Support: The contractor shall provide user experience support and consultation for web sites, tools, and apps. This will include supporting development of wireframes, information architectures, and taxonomies, perform Usability Expert (UX) reviews on existing products and perform usability testing on new products and pages. User interfaces shall be created by incorporating user experience research, light weight usability studies, requirements, and a design process. The contractor will create user flows and wireframes to build user interfaces, mockups, and prototypes, and design across multiple device types (such as desktop and mobile including tablets and smartphones) and platforms (iPhone Operating System [iOS], Android, Windows, etc.). Deliverables, recommendations and work products must support and incorporate CDC's standard templates, responsive design, and digital first design principles.

2.7 Graphic Design: The contractor shall provide advanced level graphical support to create a variety of graphic elements to enhance health messages and branding of digital content related to web pages, and associated campaign materials, and social media platforms. Graphical elements will include, but not limited to: motion graphics illustrations, infographics, special-effects elements, internal branding images, web buttons and banners, and e-mail newsletters and other communications, including those to support Task 3. The contractor must ensure all graphics adhere to 508 compliancy, CDC branding, copyright, and other rules and regulations for creation of all graphics. Contractors must be well versed in Adobe Creative Suite and related graphical software and tools to create, edit, and maintain graphic products and be able to resize and adjust pixels for identified platform and use in other channels.

TASK 3: DIGITAL MEDIA CONTENT MANAGEMENT: Support for this task will focus on digital media content development and management for NCIRD social media. The current NCIRD digital media

portfolio consists of multiple channels (see Appendix A for full list of profiles owned and supported). The number and use of these channels may vary, based on NCIRD and agency needs each year, especially in the event of a public health emergency (see Optional TASK 5).

The contractor shall provide development and coordination of digital media content and graphic assets, day-to-day handling of NCIRD social media accounts, and evaluation of digital media activities. The contractor will:

a. Support development of digital media strategies, tactics, and execute plans, consulting with NCIRD staff on communication needs and digital channels.
b. Use existing and research and evaluate emerging technology, tools and platforms for digital media channels, including social media apps, blogs, microblogs, and other digital features.
c. Work with NCIRD SMEs to create, update, and edit content for social media channels. Coordinate feedback and approvals.
d. Coordinate scheduling of social media and dissemination for optimum reach and engagement, as well as promote other tools which shall include, but are not limited to, buttons, badges, widgets, podcasts, interactive web applications , and quizzes.
e. Identify and evaluate suitability of existing and emerging digital media channels and tools; create user profiles and personas for use of those channels.
f. Identify ongoing top tasks for NCIRD's audiences and recommend ways to make the digital media interaction more informative and satisfying for end users, following CDC Digital First principles and usability guidelines.
g. Provide proven strategies and tactics to increase audience share for, and engagement with, NCIRD's digital media messages and tools.
h. Perform ongoing formal evaluation of digital media activities, supplemented with data from NCIRD-licensed tools (e.g., Adobe Analytics, Sprout Social, and Meltwater), assemble and share reports, and provide recommendations for the most effective use of these resources.
i. Ensure that all digital media tools and activities comply with Federal, HHS and CDC rules and standard including Section 508.

C4 DELIVERABLES: All task order deliverables intended for communication to the public must comply with Public Law 111–274, the Plain Writing Act of 2010. For Plain Language, information and the Federal Plain Language Guidelines see www.plainlanguage.gov.

All reports shall be submitted to the COR and Technical Monitor electronically in accordance with the delivery scheduled below and as determined by CDC.

Deliverable	Delivery Method	Frequency /Date	Deliver To
Kick-off Meeting	Conference Call	02/21/21	COR or Technical Monitor
Workplan	Electronically to COR and Discussed in regular meeting(s)	02/21/21	
Active Projects Report		Weekly	
Completed Project Report		10 days after completion	
Estimate at Completion (EAC) Cost Report		Monthly	
Staffing and Project Information Maintained in JIRA			
Physical Equipment /Software Product Inventory		Bi-Annually	
Cost and Schedule Baselines	EPLC SharePoint site	Real Time	
Transition Out Plan	Electronically to COR	01/15/24	

C5 PERIOD OF PERFORMANCE: This contract shall be for a perind of not to exceed three (3) years. This includes one (1) base year and two (2) optional years.
Base year: February 15, 2021 - February 14, 2022
Option 1: February 15, 2022 - February 14, 2023
Option 2: February 15, 2023 - February 14, 2024

Anticipated hours of operation are 8:30 a.m. – 5:00 p.m., Monday through Friday. In order to support urgent work, after hours support may be required. The contractor shall provide, when requested, on-call support for all

nights and weekends for emergency web postings and respond to any request within three (3) hours. For example, if there was an emergency involving one of the supported websites, the contractor may be asked to provided shift coverage for nights and weekends.

C6 PLACE OF PERFORMANCE: The contractor shall perform the work with a combination of onsite at CDC facilities and offsite at the contractor's facility. The following is a breakdown of which labor categories have historically worked onsite and offsite. Given the current COVID environment and extended telework provisions at CDC, all resources may need to perform work offsite for at least the beginning of contract performance.

OnSite Support
Labor Category
Business Systems Analyst II
Computer Prog. II
Computer Prog. III
Project Control Specialist
Technical Info. Spec.
User Relations Spec.
Web Designer

OffSite Support
Labor Category
Computer Prog. II
Public Health Analyst II
Strategic Planner
Systems Analyst II
Technical Info. Spec.
User Relations Spec.

C7 GOVERNMENT FURNISHED PROPERTY: CDC will provide workspace, IT equipment (i.e., desktop computer), telephone, key fob, and other office equipment and supplies as necessitated by the work requirements. Access to CDC IT systems and facilities will be controlled through use of CDC-issued HSPD-12 compliant ID badge. The contractor, as an independent party and not as an agent of the Government, shall provide all labor and supervision to perform the services specified.

C8 TRAVEL: Non local travel is not anticipated for this requirement.

C9 TELEWORK: Telework is available at the discretion of the contractor and approval of the Contracting Officer. A contractor must submit their telework policy to the contracting officer for approval. Teleworking may be available in the event of facilities closure (e.g., emergency closure, weather-related events, etc.). Telework will be governed by the same rules and policies in effect at the onsite work location. The tour of duty for telework should reflect the regular workday schedule of the teleworker, with exceptions negotiated by and authorized by the COR

C10 MINIMUM VENDOR QUALIFICATIONS: To achieve tasks, contracted staff must have expert knowledge and understanding of web services and digital media that will allow the vendor to support this critical work for CDC.

Special Knowledge Skills and Abilities Required of Contractor Personnel:

1. Expert knowledge of developing, implementing, and supporting digital IT services and products, including website, web application, and digital social media technologies and platforms
2. Substantial experience with designing, developing, and managing digital web content, and with the associated or underlying science for immunization and respiratory diseases (e.g. AFM, Legionnaires, meningitis, etc.)
3. In-depth knowledge and experience collaborating with immunization-based and public health organizations and partners on digital IT services, such as ACIP, State and local health departments, MenAfriNet, etc.

C11 PERFORMANCE MATRIX

TASKS	Acceptable Quality Level (AQL) for ALL TASKS 100%	Method	Incentives/ Disincentives
Project Management	Workplan includes recurring meetings, deliverables, deadlines and milestones	s (by the report w of	- Contractor's performance is documented as past

Website Support Services Digital Media Content Management	Activities are conducted and products are delivered within established timeframe and as outlined in the PWS		performance using CPARS which is considered for future awards. - Performance is considered in determining whether to exercise the option periods. - Repeated complaints will be elevated for higher level resolution (senior management and/or OAS)
	Benchmarks set and met for specific activities		
	Requests from NCIRD units are reviewed and completed in accordance with the level of service agreement (Appendix A)		
	System functionality is monitored and updated as necessary and outlined in the PWS		
	Content is appropriate and technically accurate		
	Products encompass all QA standards, Accessibility and SEO		
	Activities and products adhere to CDC policy, guidelines, standards, best practices, and federal laws		

C12 SPECIAL REQUIREMENT

Paper Reduction Act:
"The Paperwork Reduction Act of 1995 (PRA): Offerors should be advised that any activities involving information collection (i.e., posing similar questions or requirements via surveys, questionnaires, telephonic requests, focus groups, etc.) from 10 or more non-Federal entities/persons, including States, are subject to PRA requirements and may require CDC to coordinate an Office of Management and Budget (OMB) Information Collection Request clearance prior to the start of information collection activities. This would also include information sent to or obtained by CDC via forms, applications, reports, information systems, and any other means for requesting information from 10 or more persons; asking or requiring 10 or more entities/persons to keep or retain records; or asking or requiring 10 or more entities/persons to disclose information to a third-party or the general public."

CAPITAL PLANNING AND INVESTMENT CONTROL/PROJECT MANAGEMENT
The Federal Government mandates the prudent management of IT investments. Capital planning and Investment Control (CPIC) is a continuous and integrated process for managing the risk and returns if information technology (IT) investments. The CPIC process fully integrates with the CDC's overall budget, finance, acquisition, strategic planning, enterprise architecture, security, and other relevant processes. CPIC also aligns with DHHS Enterprise Performance Life Cycle (EPLC) framework and is used for all IT related decisions.

The contractor will follow the EPLC framework, which will provide a standard structure for planning, managing, and overseeing IT projects over their entire life cycle. The framework consists of ten life cycle phases. Within each phase, activities, responsibilities, reviews and deliverables are defined/ Templates for the deliverables are available to the contractor after award. Exit criteria are established for each phase and Stage Gate reviews are conducted through CDC's IT Governance process to ensure that the project's management quality, soundness, and technical feasibility remain adequate and the project is ready to move forward to the next phase. All IT projects in support of this task must adhere to the EPLC requirements and pass each State Gate as appropriate. More information about EPLC can be found at https://www.hhs.gov/web/governance/digital-strategy/it-policy-archive/policy-for-information-technology-enterprise-performance.html

DATA CLAUSE
a. Data Collection and Monitoring
The contractor shall provide ongoing support for collecting quantitative and qualitative data and conducting related data management processes. The contractor shall continuously improve the development, organization, and maintenance of processes for data collection, monitoring, and related data management activities.
b. Data Quality
The contractor shall ensure that data/datasets provide the highest data quality possible and are suitable for their intended uses in decision making, planning, and operations. The dimensions of data quality include, but are not limited to, accuracy, completeness, consistency, currency, precision, privacy, timeliness, and validity. Each sub-task below should contribute to improving data quality.

To ensure data quality, the contractor shall provide routine and ongoing data quality–monitoring, control, assurance, improvement, and oversight– for (1) national- and local-level data submitted to CDC, (2) data and datasets generated from CDC studies, and (3) any other CDC-managed data. The contractor shall also ensure data quality for all deliverables such as accurate and complete data management documentation, tracking information, and data tables, summaries, reports, presentations, etc.

STATEMENT OF WORK

Title: Evaluating School Strategies for COVID-19 Mitigation

SECTION 1—BACKGROUND

Schools are an important part of the infrastructure of communities, as they provide safe, supportive learning environments for students and also help mitigate health disparities by providing critical services such as school meal programs and social, physical, behavioral, and mental health services. As community transmission of COVID-19 was emerging in the United States in early 2020, schools across the country faced difficult decisions about how to best educate students while protecting the health of students and staff, as well as supporting community-wide efforts to lower transmission and reduce strain on healthcare infrastructure. Widespread school closures were implemented in Spring 2020, but by the beginning of the 2020-2021 school year, schools across the country had developed more refined approaches for a return to learning, with most state and local education agencies drawing heavily from CDC guidance on COVID-19 mitigation in schools.

Schools that offered, or plan to offer, in-person instruction have implemented numerous additional strategies to reduce the risk of COVID-transmission. These strategies, typically grounded in CDC's "Considerations" for operating schools during COVID-19, have included strategies for promoting behaviors that reduce COVID-19's spread, maintaining healthy environments, maintaining healthy operations, and preparing for when someone gets sick. Commonly implemented approaches have included requiring or recommending face masks, modifying layouts and traffic patterns to increase physical distance between students and staff, supporting improved hand hygiene and cough etiquette practices, improving ventilation, and enhancing cleaning and disinfection.

To better respond throughout the life of the current COVID-19 pandemic and to inform responses to outbreaks of similar infectious diseases in the future, the Government seeks to better understand the relationships between mitigation strategies used by schools to reduce COVID-19 transmission and the context of COVID-19 cases and transmission in those schools and their communities. This delivery order will provide support to conduct a largescale study to examine these relationships, using both existing data sources and new data collections to compile a comprehensive dataset with longitudinal data points at state, local education agency (school district), and school levels.

SECTION 2 – PURPOSE

The goal of this requirement is to build on CDC's network of funded state education agencies (SEA) and local education agencies (LEA) to answer questions about the feasibility and effectiveness of CDC school mitigation strategies and associations with COVID-19 transmission.

This requirement seeks to (1) document the types of COVID-19 mitigation strategies in school district plans and track changes in these over time, (2) understand which strategies (number and type) have been and are being implemented, the extent to which they are successfully implemented at the school level, and what types of barriers and facilitators impact their implementation, and (3) describe the relationship between COVID-19 school mitigation strategies and cases of COVID-19 reported in those schools and in the schools' surrounding communities. CDC will use study findings to inform refinements to CDC's COVID-19 mitigation guidance and technical assistance for schools.

The specific objectives of this requirement are:

1. Conduct an evaluation study to explore COVID-19 mitigation strategies in schools and the relationship of these strategies to COVID-19 cases and transmission in the schools and their communities.
2. Provide the Government with a dataset that links primary and secondary data on school, district, and state education agency strategies for COVID-19 mitigation to indicators of COVID-19 cases and transmission in schools and their communities.

3. Summarize and disseminate findings related to relationships between key school-based COVID-19 mitigation approaches and school- and community-level COVID-19 indicators.

SECTION 3 – TASKS TO BE PERFORMED

The Contractor shall conduct an evaluation study to explore COVID-19 mitigation strategies in schools and the relationship of these strategies to COVID-19 cases and transmission in the schools and their communities.

This requirement includes a base task (for collecting, analyzing, and reporting data from the 2020-2021 school year) and an optional task (for collecting, analyzing, and reporting data from the 2021-2022 school year). Each of those include the following critical sub-tasks: developing an evaluation plan; collecting, compiling, and managing all data for the study; analyzing data; summarizing and disseminating findings; and engaging in ongoing communication with the Government.

The evaluation is expected to answer the following key questions:

1. What mitigation strategies do school districts include in their plans for reducing COVID-19 transmission within schools? *(captures documented policy)*
2. What mitigation strategies (number, type, cost, and extent of implementation) are schools using to reduce COVID-19 transmission within schools? *(captures implementation of the strategies in the policy and anything that may go beyond the policy)*
3. What are the barriers and facilitators to effective implementation of these mitigation strategies?
4. How does the implementation of mitigation strategies relate to COVID-19 cases within the school and community?

The study shall be designed around a sample of state education agencies (SEAs), a corresponding sample of select local education agencies (LEAs) within those states, and a sample of schools from within those districts. All DASH-funded districts in a selected state shall be included in the study, but additional districts (selected in coordination with SEA officials) shall also be selected for inclusion. The Contractor shall determine the appropriate number of school districts and schools for inclusion using power calculations to determine the sample size necessary to provide key findings and support desired analyses.

An initial selection of states, outlined in Table 1, is provided in order to capture variation in mitigation approaches in use as well as geographic region. The contractor shall prioritize these states for inclusion in the study, but is not limited to only these states. The sample of states (and associated districts and schools) shall be selected to offer geographic variation and both schools that did and schools did not begin the 2020-2021 school year with in-person instruction. The sample of school districts and schools shall be purposefully drawn to provide variation in mitigation approaches, community transmission levels of COVID-19 (including counties with lower transmission levels and those that are persistent areas of concern), racial and ethnic diversity of students, and rural, urban, and suburban settings. Included school districts shall include both CDC-funded and non-CDC-funded LEAs. Priority state and local education agencies are listed in Table 1, but the contractor design is not limited to these states and districts.

Table 1. Priority state and local education agencies for inclusion in the study.

Proposed State and Local Education Agencies for Inclusion	
State Education Agencies (SEAs)	**Local Education Agencies (LEAs)**
Arkansas*	Districts to be determined
California	Los Angeles Unified School District† Oakland Unified School District†

	San Diego Unified School District† San Francisco Unified School District† Additional districts to be determined
Florida	Broward County Duval County† Hillsborough County† Orange County† Palm Beach County† Pasco County† Additional districts to be determined
Massachusetts*	Boston† Additional districts to be determined
Michigan	Eaton† Genesee† Additional districts to be determined
Minnesota*	Districts to be determined
New Mexico*	Albuquerque† Additional districts to be determined
North Carolina*	Gaston County† Additional districts to be determined
Oklahoma*	Districts to be determined
Oregon*	Portland† Additional districts to be determined
Tennessee*	Nashville† Shelby County† Additional districts to be determined
Washington*	Seattle† Additional districts to be determined

*Receives funding from CDC's Division of Population Health/School Health Branch
†Receives funding from CDC's Division of Adolescent and School Health

The contractor shall perform the following tasks:

Base Task (CLIN 0001)

The base task includes development and implementation of a study of COVID-19 mitigation strategies used in schools in the 2020-2021 school year and their relationships with indicators of COVID-19 transmission.

Task 1. Develop an evaluation plan.

1.1 The Contractor shall develop an evaluation plan that includes evaluation questions, proposed district and school samples (which sample size determined based on study design, analyses of interest, and any necessary power calculations), variables of interest, data collection procedures, analysis plans, and a proposed timeline of activities. This plan (a draft and a final version) shall be provided to the COR for review and approval. Feedback from the Government shall be incorporated into the plan. The proposed sample shall include at least 12 states, with priority given to the states listed in Table 1.

The Contractor shall make every effort to include all DASH-funded districts within each included state (these are listed in Table 1), but the sample shall not be limited to DASH-funded districts. Additional districts shall be selected to increase the variation captured in mitigation strategies (and also in corresponding community transmission levels), improving the likelihood of successfully understanding how different strategies may be associated with varying levels of COVID-19 transmission. Within each included school district, the contractor shall identify a sample of schools for inclusion, stratified by elementary, middle, and high school levels. The Contractor shall also ensure representation of students and communities that may be at disproportionate risk for negative outcomes from COVID-19; this may include stratified or purposeful sampling, as well as oversampling.

1.2 The Contractor shall select and/or create and test quantitative and/or qualitative data collection instruments as necessary for the study. Where feasible, the Contractor shall prioritize use of data collection instruments currently used in COVID-19 related studies for the same populations.

1.3 The Contractor shall identify and obtain any necessary approvals for the evaluation to meet the requirements of the Government, the Contractor, and the selected participating education agencies. Submit approvals to the COR per the deliverables table. Approvals shall include Office of Management and Budget (OMB), Institutional Review Board (IRB), and school district-specific approvals. The Contractor shall directly obtain many approvals (e.g., IRB, school-district specific approvals); for others, such as OMB, the Contractor shall complete all documentation and monitor progress while the Government ushers materials through the approval process. The Government anticipates that an OMB waiver can be used for this COVID-19-related study; in this case, the required OMB approval shall be documentation of the waiver.

1.4 The Contractor shall coordinate the evaluation plan to the extent possible with other on-going COVID-19 related data collection efforts at the Centers for Disease Control and Prevention, selected states, and localities. The Contractor shall identify any additional COVID-19 related data collection efforts with which to coordinate.

Task 2. Collect, compile, and maintain data. Data shall be longitudinal in nature, with repeated measures or data points within districts and schools throughout the 2020-2021 school year, including retrospective data from the portion of the school year that has already passed.

2.1 The Contractor shall implement procedures to ensure and maintain confidentiality of the data, if applicable. Submit a copy of these procedures to the COR in accordance with the deliverables table. This plan shall be aligned with any CDC information technology security requirements. The Contractor is not expected to gather personally identifiable information related to any COVID-19 cases or their contacts. Case and contact data are expected to be deidentified prior to collection.

2.2 The Contractor shall coordinate and conduct primary data collection in a manner that provides quality assurance and remains consistent with the evaluation plan. Data collection may include use of paper-pencil questionnaires, web-based questionnaires, in-person interviews, focus groups, observation, and document review and abstraction.

2.3 The Contractor shall collect and compile all necessary secondary data. This shall be done in a manner that provides quality assurance and remains consistent with the evaluation plan/study design. Data sources may include federal, state and local education agencies, schools, state and local health departments, and other repositories of COVID-19 or school policy data. Collection of secondary data may require submitting data requests or compiling data from publicly available sources (e.g., health department or education agency websites).

2.4 The Contractor shall develop and implement a system for linking and maintaining data. Data from multiple sources shall be linked in a comprehensive dataset. For example, data from a state education agency would be linked to the data for districts and schools in that state; data for a school district or school would be linked to community transmission indicators in the district or school's community.

2.5 The Contractor shall develop and implement a data sharing plan for sharing compiled datasets with the Government on an ongoing basis (e.g., either as updates are made in real time or at regular intervals following new data collections and based on timing outlined in the evaluation plan). This

plan (both a draft and final version) shall be reviewed and approved by the COR. Any feedback from the Government shall be incorporated into the plan. The initial compiled dataset shall be shared with the COR within 1 month of creation, and a final dataset shall be shared with the COR when data collection is complete.

2.6 The Contractor shall develop documentation (e.g., a data dictionary) to facilitate use of the compiled dataset.

2.7 If in-person data collection is necessary, the Contractor shall make necessary arrangements to travel or the purpose of data collection. Any travel must be authorized by the COR in advance.

Task 3. Analyze evaluation data.

3.1 The Contractor shall assure that the data are accurate and consistent, appropriately and accurately linked and de-identified, and any variables or scales are constructed as outlined in the approved evaluation plan.

3.2 The Contractor shall conduct data analyses outlined in the approved evaluation plan. The Contractor shall submit any changes to the planned analyses to the Government for approval before proceeding.

Task 4. Disseminate evaluation findings with the review and approval of the COR.

4.1 Once data analyses begin, the Contractor shall provide weekly updates to the COR.

4.2 The Contractor shall provide quarterly reports of ongoing data analyses and preliminary or emerging findings by the end of the 3rd, 6th, and 9th months.

4.3 The contractor shall provide a draft and final, overall summary report of findings for the Government and participating agencies (e.g., participating state education agencies, local education agencies). This report shall include a summary of the methods of the study.

4.4 The Contractor shall develop materials, both a draft and final version, to present study information and findings to Government and non-Government audiences.

4.5 The Contractor shall provide at least one (1) manuscript, both a draft and final version, suitable for peer-reviewed publication to the COR.

Task 5. Communicate with the Government on an on-going basis.

5.1 The Contractor shall attend one virtual kick-off meeting with CDC staff within the first month of award of the contract to discuss the study and plan for all tasks. The Contractor shall provide a meeting agenda to the COR within the first 2 weeks following contract award.

5.2 The Contractor shall provide a written summary of all meeting(s) with the Government, including the kickoff meeting.

5.3 The Contractor shall communicate with the Government about study progress through phone, e-mail, web conferencing, and/or other methods of communication on a regular (e.g., weekly) basis.

Option Task (CLINs 1001 and 1002)

The option task includes the development and implementation of a study of COVID-19 mitigation strategies used in schools in the 2021-2022 school year and their relationships with indicators of COVID-19 transmission. It is anticipated that these tasks shall build on the infrastructure and documentation developed for the Base Task where possible.

Task 6. Revise the evaluation plan from the base task.

6.1 The Contractor shall revise the evaluation plan from the base task as necessary to incorporate data collection for the 2021-2022 school year. The plan shall include any updates to the evaluation questions, prioritized district and school samples, variables of interest, data collection procedures,

analysis plans, and a proposed timeline of activities. This plan shall be reviewed and approved by the COR. Feedback from the Government shall be incorporated into the plan.

6.2 The Contractor shall select and/or create/revise, and test quantitative and/or qualitative data collection instruments as necessary for the study. Where feasible, the Contractor shall prioritize use of data collection instruments currently used in COVID-19 related studies for the same populations.

6.3 The Contractor shall identify and obtain any necessary approvals for the evaluation to meet the requirements of the Government, the Contractor, and the selected participating agencies. Approvals shall include OMB, IRB, and school district-specific approvals. The Contractor shall directly obtain many approvals (e.g., IRB, school district specific approvals); for others, such as OMB, the Contractor shall complete all documentation and monitor progress while the Government ushers materials through the approval process. The Government anticipates that an OMB waiver can be used for this COVID-19-related study; in this case, the required OMB approval shall be documentation of the waiver.

6.4 The Contractor shall continue to coordinate the evaluation plan to the extent possible with other on-going COVID-19 related data collection efforts at the Centers for Disease Control and Prevention, selected states, and localities. The Contractor shall identify any additional COVID-19 related data collection efforts with which to coordinate.

Task 7. Collect, compile, and maintain data. Data are expected to be longitudinal in nature, with repeated measures or data points within districts and schools throughout the 2021-2022 school year, including retrospective data from any portion of the school year that may have already passed at the time the option is exercised.

7.1 The Contractor shall implement procedures to ensure and maintain confidentiality of the data, if applicable. This plan shall be aligned with any CDC information technology security requirements. The Contractor is not expected to gather personally identifiable information related to any COVID-19 cases or their contacts. Case and contact data are expected to be de-identified prior to collection.

7.2 The Contractor shall coordinate and conduct primary data collection in a manner that provides quality assurance and remains consistent with the evaluation plan. Data collection may include use of paper-pencil questionnaires, web-based questionnaires, in-person interviews, focus groups, observation, and document review and abstraction.

7.3 The Contractor shall collect and compile all necessary secondary data. This shall be done in a manner that provides quality assurance and remains consistent with the evaluation plan/study design. Data sources may include federal, state and local education agencies, schools, state and local health departments, and other repositories of COVID-19 or school policy data. Collection of secondary data may require submitting data requests or compiling data from publicly available sources (e.g., health department or education agency websites).

7.4 The Contractor shall develop and implement a system for linking and maintaining data. Data from multiple sources shall be linked in a comprehensive dataset. For example, data from a state education agency would be linked to the data for districts and schools in that state; data for a school district or school would be linked to community transmission indicators in the district or school's community.

7.5 The Contractor shall develop and implement a data sharing plan for sharing compiled datasets with the Government on an ongoing basis (e.g., either as updates are made in real time or at regular intervals following new data collections and based on timing outlined in the evaluation plan). This plan shall be reviewed and approved by the COR. Any feedback from the Government shall be incorporated into the plan. The initial compiled dataset shall be shared with the COR within 1 month of creation, and a final dataset shall be shared with the COR when data collection is complete.

7.6 The Contractor shall develop documentation (e.g., a data dictionary) to facilitate use of the compiled dataset.

7.7 If in-person data collection is necessary from Contractor staff, the Contractor shall make necessary arrangements to travel for the purpose of data collection. Any travel must be authorized by the COR in advance.

Task 8. Analyze evaluation data.

8.1 The Contractor shall assure that the data are accurate and consistent, appropriately and accurately linked and de-identified, and any variables or scales are constructed as outlined in the approved evaluation plan.

8.2 The Contractor shall conduct data analyses outlined in the approved evaluation plan. The Contractor shall submit any changes to the planned analyses to the Government for approval before proceeding.

Task 9. Disseminate evaluation findings with the review and approval of the COR.

9.1 Once data analyses begin, the Contractor shall provide weekly updates to the COR.

9.2 The Contractor shall provide quarterly reports of ongoing data analyses and preliminary or emerging findings by the end of the 3rd, 6th, 9th, 12th, and 15th months.

9.3 The contractor shall provide a final, overall summary report of findings for the Government and participating agencies (e.g., participating state education agencies, local education agencies). This report shall include a summary of the methods of the study.

9.4 The Contractor shall develop materials to present study information and findings to Government and non-Government audiences.

9.5 The Contractor shall provide at least one (1) manuscript suitable for peer-reviewed publication to the COR.

Task 10. Communicate with the Government on an on-going basis.

10.1 The Contractor shall attend one virtual kick-off meeting with CDC staff within the first month of the start of the option task period of performance to discuss the study and plan for all tasks. The Contractor shall provide a meeting agenda to the COR within the first 2 weeks following the start of the option task period of performance.

10.2 The Contractor shall provide a written summary of all meeting(s), including the kick off meeting for the option task.

10.3 The Contractor shall communicate with the Government about study progress through phone, e-mail, web conferencing, and/or other methods of communication on a regular (e.g., weekly) basis.

Option Task 2 (CLINs 2001 and 2002)

Option task 2 includes the expansion of the study of COVID-19 mitigation strategies used in schools in the 2021-2022 school year and their relationships with indicators of COVID-19 transmission. Specifically, this expansion shall support the inclusion of approximately 1000 additional schools (for a total size of approximately 1600 schools) in the study sample for the 2021-2022 school year. This task shall build directly on, and be integrated into, the infrastructure and documentation developed for the Option Task. Specifically, the expanded sample of an additional 1000 schools shall be integrated into the ongoing Option Task study sample. Deliverables for the Option Task and for Option Task 2 shall be combined (for example, an evaluation report of findings will report on data collected under the Option Task and Option Task 2 as a single aggregate set of data).

Task 11. Revise the evaluation plan from the base task.

11.1 The Contractor shall revise the Option Task evaluation plan, as needed, to incorporate expanded data collection for the 2021-2022 school year. The plan shall include approximately 1000 additional schools in the sample, as well as any updates to the evaluation questions, variables of interest, data collection procedures, analysis plans, and a proposed timeline of activities. This plan shall be reviewed and approved by the COR. Feedback from the Government shall be incorporated into the plan.

11.2 The Contractor shall select and/or create/revise, and test quantitative and/or qualitative data collection instruments as necessary for the study. Where feasible, the Contractor shall prioritize use of data collection instruments currently used in COVID-19 related studies for the same populations.

11.3 The Contractor shall identify and obtain any necessary approvals for the evaluation to meet the requirements of the Government, the Contractor, and the selected participating agencies. Approvals shall include OMB, IRB, and school district-specific approvals. The Contractor shall directly obtain many approvals (e.g., IRB, school district specific approvals); for others, such as OMB, the Contractor shall complete all documentation and monitor progress while the Government ushers materials through the approval process. The Government anticipates that an OMB waiver can be used for this COVID-19-related study; in this case, the required OMB approval shall be documentation of the waiver.

11.4 The Contractor shall continue to coordinate the evaluation plan to the extent possible with other on-going COVID-19 related data collection efforts at the Centers for Disease Control and Prevention, selected states, and localities. The Contractor shall identify any additional COVID-19 related data collection efforts with which to coordinate.

Task 12. Collect, compile, and maintain data for the schools in the expanded sample. Data are expected to be longitudinal in nature, with repeated measures or data points within schools throughout the 2021-2022 school year.

12.1 The Contractor shall implement procedures to ensure and maintain confidentiality of the data, if applicable. This plan shall be aligned with any CDC information technology security requirements. The Contractor is not expected to gather personally identifiable information related to any COVID-19 cases or their contacts. Case and contact data are expected to be de-identified prior to collection.

12.2 The Contractor shall coordinate and conduct primary data collection in a manner that provides quality assurance and remains consistent with the evaluation plan. Data collection may include use of paper-pencil questionnaires, web-based questionnaires, in-person interviews, focus groups, observation, and document review and abstraction. Survey data collection shall include the expanded sample of schools in order to ensure sufficient response to support data analysis.

12.3 The Contractor shall collect and compile all necessary secondary data. This shall be done in a manner that provides quality assurance and remains consistent with the evaluation plan/study design. Data sources may include federal, state and local education agencies, schools, state and local health departments, and other repositories of COVID-19 or school policy data. The Contractor is expected to collect secondary data (e.g., school COVID case counts, community COVID transmission indicators, community vaccination rates) for all schools responding to the survey, and will collect at least some additional secondary data for schools in the sample that do not respond to the survey. Collection of secondary data may require submitting data requests or compiling data from publicly available sources (e.g., health department or education agency websites), and may require gathering data on a school-by-school, district-by-district, or state-by-state basis.

12.4 The Contractor shall develop and implement a system for linking and maintaining data. Data from multiple sources shall be linked in a comprehensive dataset. For example, data from a state education agency would be linked to the data for districts and schools in that state; data for a school district or school would be linked to community transmission indicators in the district or school's community.

12.5 The Contractor shall develop and implement a data sharing plan for sharing compiled datasets with the Government on an ongoing basis (e.g., either as updates are made in real time or at regular intervals following new data collections and based on timing outlined in the evaluation plan). This plan shall be reviewed and approved by the COR. Any feedback from the Government shall be incorporated into the plan. The initial compiled dataset shall be shared with the COR within 1 month of creation, and a final dataset shall be shared with the COR when data collection is complete.

12.6 The Contractor shall develop documentation (e.g., a data dictionary) to facilitate use of the compiled dataset.

12.7 If in-person data collection is necessary from Contractor staff, the Contractor shall make necessary arrangements to travel for the purpose of data collection. Any travel must be authorized by the COR in advance.

Task 13. Analyze evaluation data.

13.1 The Contractor shall assure that the data are accurate and consistent, appropriately and accurately linked and de-identified, and any variables or scales are constructed as outlined in the approved evaluation plan.

13.2 The Contractor shall conduct data analyses outlined in the approved evaluation plan. The Contractor shall submit any changes to the planned analyses to the Government for approval before proceeding.

Task 14. Disseminate evaluation findings with the review and approval of the COR.

14.1 Once data analyses begin, the Contractor shall provide weekly updates to the COR.

14.2 The Contractor shall provide quarterly reports of ongoing data analyses and preliminary or emerging findings within the quarterly reports submitted for the Option Task. Data from the Option Task and Option Task 2 will be presented in aggregate.

14.3 The contractor shall provide a final, overall summary report of findings for the Government and participating agencies (e.g., participating state education agencies, local education agencies). This report shall include a summary of the methods of the study. This report will include data from the Option Task and Option Task 2 presented in aggregate.

14.4 The Contractor shall develop materials to present study information and findings to Government and non-Government audiences.

14.5 The Contractor shall provide at least one (1) manuscript suitable for peer-reviewed publication to the COR. This manuscript will include data from the Option Task and Option Task 2 presented in aggregate.

Task 15. Communicate with the Government on an on-going basis.

15.1 The Contractor shall provide a written summary of all meeting(s).

15.2 The Contractor shall communicate with the Government about study progress through phone, e-mail, web conferencing, and/or other methods of communication on a regular (e.g., weekly) basis.

SECTION 4 – GOVERNMENT FURNISHED MATERIALS

The contractor may need to obtain access to the Government's Intranet for the purpose of performing this requirement. The contractor shall be responsible for meeting all Government security requirements to acquire this access. Upon meeting all Government security requirements for access, the Government will provide a Smart Card and Smart Card reader for contractor staff directly responsible for performing data retrieval or data transfers tasks.

SECTION 5 – DELIVERABLES/REPORTING SCHEDULE

Base Task (CLIN 001)

Task Number	Deliverable	Quantity/ Format	Deliver To	Delivery Date
1.1	Draft evaluation plan	1 copy / electronic file	COR	By the middle day of the day of the 2nd month of contract performance

1.1	Final evaluation plan			By the last day of the 2nd month of contract performance
1.2	Copies of data collection instruments	1 copy each / electronic file	COR	By the last day of the 3rd month of contract performance
1.3	Documentation that required approvals have been secured or are in process	1 copy / electronic file	COR	By the last day of the 4th month of contract performance
2.1	Written description of procedures to ensure and maintain confidentiality of data (may be provided in IRB or OMB approval materials)	1 copy / electronic file	COR	By the last day of the 4th month of contract performance
2.5	Draft written data sharing plan for submitting compiled datasets	1 copy / electronic file	COR	By the last day of the 4th month of contract performance
2.5	Final written data sharing plan for submitting compiled datasets	1 copy / electronic file	COR	By the middle day of the 5th month of contract performance
2.5	Initial compiled dataset	1 copy / electronic file	COR	Within 1 month of initial data compilation
2.5	Final compiled dataset including written documentation to facilitate use of the dataset (e.g., data dictionary)	1 copy / electronic file	COR	By last day of the 12th month of contract performance
4.1	Weekly update	1 copy / email	COR	Before the Friday of each week at noon
4.2	Description of data analysis progress in the 3-, 6- and 9-month reports	1 copy / electronic files	COR	By the last day of the 3rd, 6th, and 9th months of contract performance
4.3	Draft, overall summary report of methods and findings	1 copy / electronic file	COR	By the middle day of the 11th month of contract performance
4.3	Final, overall summary report of methods and findings	1 copy / electronic file	COR	By the last day of the 12th month of contract performance
4.4	Draft presentation materials	1 copy / electronic files (e.g., PowerPoint slides, handouts, speaker's notes)	COR	By the middle day of the 11th month of contract performance

4.4	Final presentation materials	1 copy / electronic files (e.g., PowerPoint slides, handouts, speaker's notes)	COR	By the last day of the 12th month of contract performance
4.5	Draft of manuscript for peer-reviewed publication	1 copy / electronic file	COR	By the middle day of the 11th month of contract performance
4.5	Final manuscript for peer-reviewed publication	1 copy / electronic file	COR	By the last day of the 12th month of contract performance
5.1	Agenda for kick off meeting	1 copy / electronic file	COR	By last day of 2nd week of contract performance
5.1, 5.2, 5.3	Written summary of any meetings with the Government	1 copy / electronic files	COR	Within 7 days of each meeting

Option Task (CLINs 1001 and 1002)

Task Number	**Deliverable**	**Quantity/ Format**	**Deliver To**	**Delivery Date**
6.1	Draft evaluation plan	1 copy / electronic file	COR	By the middle day of the day of the 2nd month of contract performance
6.1	Final evaluation plan			By the last day of the 2nd month of contract performance
6.2	Copies of data collection instruments	1 copy each / electronic file	COR	By the last day of the 3rd month of contract performance
6.3	Documentation that required approvals have been secured or are in process	1 copy / electronic file	COR	By the last day of the 4th month of contract performance
7.1	Written description of procedures to ensure and maintain confidentiality of data (may be provided in IRB or OMB approval materials)	1 copy / electronic file	COR	By the last day of the 4th month of contract performance
7.5	Draft written data sharing plan for submitting compiled datasets	1 copy / electronic file	COR	By the last day of the 4th month of contract performance
7.5	Final written data sharing plan for submitting compiled datasets	1 copy / electronic file	COR	By the middle day of the 5th month of contract performance

7.5	Initial compiled dataset	1 copy / electronic file	COR	Within 1 month of initial data compilation
7.5	Final compiled dataset including written documentation to facilitate use of the dataset (e.g., data dictionary)	1 copy / electronic file	COR	By last day of the 18th month of contract performance
9.2	Description of data analysis progress in the 3-, 6- and 9-month reports	1 copy / electronic files	COR	By the last day of the 3rd, 6th, 9th, 12th, and 15th months of contract performance
9.3	Draft, overall summary report of methods and findings	1 copy / electronic file	COR	By the middle day of the 17th month of contract performance
9.3	Final, overall summary report of methods and findings	1 copy / electronic file	COR	By the last day of the 18th month of contract performance
9.4	Draft presentation materials	1 copy / electronic files (e.g., PowerPoint slides, handouts, speaker's notes)	COR	By the middle day of the 17th month of contract performance
9.4	Final presentation materials	1 copy / electronic files (e.g., PowerPoint slides, handouts, speaker's notes)	COR	By the last day of the 18th month of contract performance
9.5	Draft of manuscript for peer-reviewed publication	1 copy / electronic file	COR	By the middle day of the 17th month of contract performance
9.5	Final manuscript for peer-reviewed publication	1 copy / electronic file	COR	By the last day of the 18th month of contract performance
10.1	Agenda for kick off meeting	1 copy / electronic file	COR	By last day of 2nd week of contract performance
10.1, 10.2, 10.3	Written summary of any meetings with the Government	1 copy / electronic files	COR	Within 7 days of each meeting

Option Task 2 (CLINs 2001 and 2002)

Task Number	**Deliverable**	**Quantity/ Format**	**Deliver To**	**Delivery Date**
11.1	Draft evaluation plan	1 copy / electronic file	COR	By the middle day of the day of the 2nd month of contract performance

11.1	Final evaluation plan			By the last day of the 2nd month of contract performance
11.2	Copies of data collection instruments	1 copy each / electronic file	COR	By the last day of the 3rd month of contract performance
11.3	Documentation that required approvals have been secured or are in process	1 copy / electronic file	COR	By the last day of the 4th month of contract performance
12.1	Written description of procedures to ensure and maintain confidentiality of data (may be provided in IRB or OMB approval materials)	1 copy / electronic file	COR	By the last day of the 4th month of contract performance
12.5	Draft written data sharing plan for submitting compiled datasets	1 copy / electronic file	COR	By the last day of the 4th month of contract performance
12.5	Final written data sharing plan for submitting compiled datasets	1 copy / electronic file	COR	By the middle day of the 5th month of contract performance
12.5	Initial compiled dataset	1 copy / electronic file	COR	Within 1 month of initial data compilation
12.5	Final compiled dataset including written documentation to facilitate use of the dataset (e.g., data dictionary)	1 copy / electronic file	COR	By last day of the 18th month of contract performance
14.2	Description of data analysis progress in the 3-, 6- and 9-month reports	1 copy / electronic files	COR	By the last day of the 3rd, 6th, 9th, 12th, and 15th months of contract performance
14.3	Draft, overall summary report of methods and findings	1 copy / electronic file	COR	By the middle day of the 17th month of contract performance
14.3	Final, overall summary report of methods and findings	1 copy / electronic file	COR	By the last day of the 18th month of contract performance
14.4	Draft presentation materials	1 copy / electronic files (e.g., PowerPoint slides, handouts, speaker's notes)	COR	By the middle day of the 17th month of contract performance
14.4	Final presentation materials	1 copy / electronic files (e.g., PowerPoint slides, handouts, speaker's notes)	COR	By the last day of the 18th month of contract performance

14.5	Draft of manuscript for peer-reviewed publication	1 copy / electronic file	COR	By the middle day of the 17th month of contract performance
14.5	Final manuscript for peer-reviewed publication	1 copy / electronic file	COR	By the last day of the 18th month of contract performance
15.1, 15.2	Written summary of any meetings with the Government	1 copy / electronic files	COR	Within 7 days of each meeting

SECTION 6 – REFERENCE MATERIALS

The following documents and/or websites provide contextual information that is relevant to the work being performed.

Background information on DASH: http://www.cdc.gov/healthyyouth

Background information on the local education agencies that received DASH funding: https://www.cdc.gov/healthyyouth/partners/funded_locals.htm

Background information on the local education agencies that received DASH funding: https://www.cdc.gov/healthyschools/fundedpartners.htm

Background information on CDC's COVID-19 guidance for schools: https://www.cdc.gov/coronavirus/2019-ncov/community/schools-childcare/index.html
https://www.cdc.gov/coronavirus/2019-ncov/community/schools-childcare/schools.html
https://www.cdc.gov/coronavirus/2019-ncov/community/schools-childcare/indicators.html
https://www.cdc.gov/coronavirus/2019-ncov/community/schools-childcare/k-12-staff.html

Performance Work Statement

Title: "Leveraging Media Coalitions to Advance Prevention Messages among Populations Disproportionately Affected by COVID-19"

I. Background and Need:

The COVID-19 pandemic continues to disproportionately affect communities of color. Data from the Centers for Disease Control and Prevention (CDC) and other public health organizations reveal stark health disparities related to COVID-19 morbidity and mortality. Black/African American. Hispanic/Latino, and American Indian/Alaska Native persons have significantly higher rates of COVID-19-related infection, hospitalization, and death compared to their White counterparts. Additionally, the COVID-19 pandemic has exacerbated other long-standing health disparities, such as the burden of chronic disease, resulting in poorer health outcomes.

Beyond these data, research also shows that racial and ethnic minority populations in the United States contend with structural and systemic barriers to care. These systemic issues are further amplified as many communities of color may have longstanding and deeply entrenched distrust of the health care system based upon personal experience and a legacy of inequity in the U.S.

While research indicates that consumers across demographics consider health care professionals among the most trusted sources of COVID-19 information, developing clear, compelling, and action-oriented messages that meet diverse audiences where they are using the most relevant communication channels has a vital role to plan in improving and informing COVID-19 public health activities. Racial and ethnic minority populations and other intersectional communities must have the information needed to persist in practicing CDC's COVID-19 prevention measures and pursue access to getting vaccinated.

Having a comprehensive, integrated, and strategic media relations strategy to reach populations disproportionately impacted by COVID-19 is integral to achieving CDC's overall health equity objectives. Leveraging media outlets that reach and resonate with these populations are critically important communication channels to reach disproportionately impacted populations. These outlets include traditional media (print, radio, broadcast), digital/online media, and podcasts. Fostering meaningful media engagements with trusted media organizations and diverse leaders will inform a culturally responsive media approach.

II. Project Objective:

The objective of this contract is to support the CDC Division of Public Affair's COVID-19 media-related health disparities and health equity activities and outreach to priority populations, to include: Audience segmentation and prioritization; media planning, outreach, and engagement; and monitoring and evaluation activities.

III. Description of Work

Task 1. Project Management

a. Kickoff Meeting - A kickoff meeting shall be held no later than 10 workdays after the initial award is made to discuss plans and timelines as well as clarify roles and responsibilities, to be held at CDC offices in Atlanta, GA.

b. Work Plan - Following the kick off meeting, the contractor shall develop a written work plan, minimally including all essential interim and final deliverables, key staff responsible for tasks (including contractor, CDC or other partners), and schedule of key deadlines (including review cycles and absolute No Later Than (NLT) dates for key activities and deliverables) for COR review and correction before acceptance. The work plan must contain:

i. a series of specific reports and activities proposed by the contractor following the kick-off meeting, to be developed by the contractor during the course of the project, inclusive of the contractor's plan for ongoing monitoring and evaluation of services to assure highly quality performance and customer satisfaction.
ii. hours of operation,
iii. contractor plan for employee management including how the contractor will avoid any appearances of personal services by the CDC, and
iv. the contractor's plan to maintain services during emergencies, such as government shutdown, building closure, inclement weather, telework, etc. or similar (infrequent) surge efforts for peak room usage for large scale events.

The work plan must be a distributable document for sharing with key CDC management/staff impacted by this project, as needed. The work plan is due no later than 10 workdays following the kickoff meeting. The work plan (and any schedule of interim deliverables) may be revised according to CDC acceptance of the updated work plan by the COR during the project with the restriction that these changes must not impact the overall period of performance, scope, or specifications of the award, or otherwise impinge on the authority of the contracting officer. It is the responsibility of the contractor to fully understand what changes require contracting officer approval.

c. Monthly Reporting – Provide a monthly report including updates on the specific reports and deliverables as described in the work plan expressly broken out. The monthly report shall be considered a substantial deliverable of the project, for review by key Center leadership as well as the project contracting officer representative, and used as 1) a tracking tool for success of this project, 2) documentation of effort/services as invoiced in the matching monthly invoice, and 3) support for need for additional incremental funding. The contractor shall develop the monthly report format for review and approval by the Contracting Officer's Representative (COR). The monthly report is due NLT than the 5th calendar day of each month.
d. Quarterly Conference Call – A quarterly conference call with CDC COR, must be held in the last two weeks of each quarter, initiated and led by the contractor. The purpose of this call is ongoing review of task performance. The discussion from the conference call must be documented in the following monthly report. Any required performance improvements must be documented/reported in the monthly reports.

Task 2. Segmentation and Prioritization

The contractor shall:

a. Develop an audience segmentation and prioritization strategy to identify target audiences and populations based on the burden of COVID-19 disease and other factors, to include geographic and race/ethnicity factors.
b. For the purposes of this contract, the strategy shall prioritize Black/African American, Hispanic/Latino, and American Indian/Alaska Native populations
c. Based on analyses, data, and best practices, identify, prioritize, and recommend target audiences for media outreach based on available public health data as well as recommend specific media outreach activities and outlets (traditional media, digital/online media, podcasts).
d. Conduct a media content analysis that examines media coverage and key messages/themes on COVID-19-related health disparities since the start of the COVID-19 pandemic. The media content analysis shall inform the overall strategy.
e. Conduct an internal rapid asset inventory of CDC communication/media activities that are designed to reach priority populations disproportionately impacted by COVID-19. The inventory shall identify existing communication and media outreach activities that are underway as well as future activities that align with the project period of performance to inform the strategy. The inventory shall identify gaps and needs related to media outreach.
f. Conduct an external analysis (e.g. SWOT) to assess the public health, communication, and media environment and to identify gaps and needs related to media outreach. The external analysis shall inform the overall strategy.

g. Conduct a review of existing literature and best practices for reaching the target audiences through media outreach and identify trusted organizations and outlets. The review shall inform the overall strategy.

Task 3. Planning, Outreach, and Engagement

The contractor shall:

a. Based on the results of Task 2, develop a media outreach and engagement strategy to reach the priority audiences using targeted media channels and strategies.
b. Articulate a media outreach approach to reach targeted populations with COVID-19 public health information.
c. Recommend key markets, media channels, organizations, and other media partnership opportunities to reach targeted populations, with a focus on digital opportunities. Identify national media opportunities as well as regional/local based on public health need where COVID-19 burden is disproportionate.
d. Engage with recommended media organizations and partners to identify opportunities to amplify CDC's COVID-19 messages across organizational and partner networks. Identify at least six (6) organizations/partners per each priority target audience.
e. Develop media materials and collateral for media organizations and partners to use in amplifying CDC's COVID-19 messages, to include but not limited to media toolkits, factsheets, digital content, videos, images, and other content.
f. Identify and implement media events and opportunities to reach targeted audiences, to include to radio media tours, roundtables, editorial boards, digital media events, media briefings, and other media activities that reach the identified priority target audiences. Secure placements and coordinate the identified activities. Conduct at least six (6) per period of performance.
g. Identify and recommend established and prospective CDC subject matter experts to serve as spokespersons for the identified media efforts. The contractor shall identify areas where media training is needed.
h. Provide a plan and conduct up to four (4) media trainings per period of performance for CDC subject matter experts to include best practices and tactics for media interviews; messaging on COVID-19 and CDC's health disparities.
i. Develop and maintain an editorial calendar of identified media outreach activities.

Task 4. Monitoring and Engagement

The contractor shall:

a. Provide a metrics monitoring plan that will measure progress toward established media objectives.
b. Within that plan recommend and establish a set of media key performance indicators (KPIs) based on industry best practices, to include standard media metrics and digital metrics such as engagement, reach, message fidelity and traction, and other quantitative and qualitative metrics.
c. Provide monthly data reports that includes data summaries as well as recommendations to inform the overall project strategy based on the data.

IV. Deliverables:

All task order deliverables intended for communication to the public must comply with Public Law 111 274, the Plain Writing Act of 2010. For Plain Language information and the Federal Plain Language Guidelines see www.plainlanguage.gov.

Item	Quantity	Delivery Method	Deliver To	Due Date
Kickoff Meeting (Task 1)	1 (per year)	Electronically via E-mail	COR and Contracting Officer	10 working days following award
Work Plan (Task 1)	1 (per year)	Electronically via E-mail	COR and Contracting Officer	10 working days following kickoff meeting
Monthly Reporting (Task 1)	12 (per year)	Electronically via E-mail	COR and Contracting Officer	Monthly by the 5th calendar day following the end of the month
Quarterly Conference Call (Task 1)	4 (per year)	Electronically via E-mail	COR and Contracting Officer	Within two weeks of end of each quarter
Audience Segmentation and Prioritization Strategy (Task 2)	1 plan	Electronically via E-mail	COR	Within 60 days post-award
Media Content Analysis (Task 2)	1 analysis	Electronically via E-mail	COR	Within 45 days post-award
Rapid Asset Inventory Analysis (Task 2)	1 analysis	Electronically via E-mail	COR	Within 45 days post-award
External Analysis (Task 2)	1 analysis	Electronically via E-mail	COR	Within 45 days post-award

Literature Review/Best Practices	1 review	Electronically via E-mail	COR	Within 45 days post-award
Media Outreach and Engagement Strategy (Task 3)	1 plan	Electronically via E-mail	COR	Within 90 days post-award
Engage with Key Media Org/Partners (Task 3)	At least 6 per audience per period of performance	Multiple	COR	90 days post-award through end of contract
Media Materials (Task 3)	As Assigned	Electronically	COR	90 days post-award through end of contract
Conduct Media Events (Task 3)	At least 6 per period of performance	Multiple	COR	90 days post-award through end of contract
Conduct Media Trainings (Task 3)	Up to 4 per period of performance	Multiple	COR	90 days post-award through end of contract
Develop and Maintain Editorial Calendar (Task 3)	1 calendar, updated at least once a month	Electronically	COR	90 days post-award through end of contract
Media Monitoring Plan (Task 4)	1 plan	Electronically	COR	Within 90 days post-award
Monthly Data Reports (Task 4)	Monthly	Electronically	COR	Monthly through end of contract upon approval of Media Monitoring Plan

All materials will be submitted electronically in MS compatible format that meets CDC standards and is readily available at CDC (e.g. MS Office (Word, Excel, PowerPoint) or Adobe Acrobat. All reporting requirements and written deliverables as part of this contract will be supplied to the project Contracting Officer Representative (COR). Acceptance of any written deliverables is pending CDC COR review and correction to any resulting comments, to be confirmed in writing and documented in the closest following monthly report. Any schedule of interim deliverables may be revised according to CDC acceptance of an updated written work plan by the COR during the project with the restriction that these changes must not impact the overall period of performance, scope, or specifications of the award, or otherwise impinge on the authority of the contracting officer. It is the responsibility of the contractor to fully understand what changes require contracting officer approval.

V. Performance Matrix:

+PERFORMANCE MATRIX (QASP)				
Desired End Result	**Standard**	**The Required Performance for Each Feature**	**Quality Assurance**	**Incentives & Payment Quality Link**

Contractor's Project Manager upholds industry project management standards and practices to ensure customer satisfaction (All Tasks)	Timeliness	Completes all actions; submits 100% of reports and documentation; and ensures ALL deliverables are provided to the agency by the due date Early identification of problems/risks and implementation of mitigation/elimination methods	COR Review Scheduled and random sampling	**Positive Incentive:** a. Payment of the contract's monthly invoice for satisfactory service. b. Contractor performance evaluated using the CPARS assessment report. The evaluation will be considered when future Agency contract selections are made. **Payment is linked to quality through, Inspection of Services:** a. The Contractor shall provide and maintain an inspection system acceptable to the Government covering services under this contract. Complete records of all inspection work performed by the contractor employees shall be maintained and made available to the Government during contract performance and for as long afterwards as the contract requires. b. If any of the services do not conform to contract requirements, the Government may require the Contractor to perform the services again in conformity with contract requirements, at no increase in contract amount. When the defects in services cannot be corrected by re-performance, the Government may (1) require the Contractor to take necessary action to ensure that future performance conforms to contract requirements and (2) reduce the contract price to reflect the reduce value of the services performed. c. If the Contractor fails to
	Execution Management	95% implementation and execution of project plan	COR Observation	
	Quality	Sufficient resource utilization of contractor employees to ensure project success; 95% effectiveness of project plan; 98% customer and stakeholder satisfaction	COR Review Customer feedback	
CDC possesses effective media relations strategies, products and materials that improve the agency's ability to provide meaningful, trustworthy information related to COVID-19 health disparities (Tasks 2, 3, and 4)	Timeliness	95% of ALL products submitted by the established due date	COR Review	
	Clarity	95% of ALL products adhere to standard grammatical, style, and writing best practices and guidelines ALL deliverables must encompass all QA standards, Accessibility, 508 compliance checks, conformance with Federal Plain Language Guidelines, and adherence to CDC policies, guidelines, standards, and best practices	COR Random Sampling 100% review by OADC	
	Quality and Consistency in Messaging	At least 95% of products/materials are accurately and consistently formatted 95% of CDC's feedback	COR Random Sampling 100% review by OADC	

		on draft content is reflected in the final product/material At least 95% of media messaging is appropriate for the subject and audience At least 95% of media messaging resonates with the CDC spokesperson's voice and/or CDC's core messages		promptly perform services again or to take necessary action to ensure future performance in conformity with contract requirements, the Government may (1) by contract or otherwise, perform the services and charge to the Contractor any cost incurred by the Government that is directly related to the performance of such services or (2) terminate the contract for default.

VI. Period of Performance:

The period of performance is:

Year 1 (Basic Period): 8-1-2021 – 7-31-2022
Year 2 (Option): 8-1-2022 – 7-31-2023

VII. Place of Performance:

Tasks can be performed offsite at the contractor's facility/remotely.

The contractor may be required to travel in support of the tasks outlined in the contract, up to four (4) trips to the CDC Atlanta campus per year. All travel must be authorized by the COR and follow the task order and all other applicable requirements.

All travel shall be in accordance with the Federal Travel Regulations (FTR) and the Joint Travel Regulations (JTR) and adhere to FAR 31.205-46. The contractor shall ensure that the requested travel costs will not exceed the amount authorized in this task order. Travel must be submitted to COR in an official request with anticipated expenses and justification.

Prior Approval: Requests for travel approval shall:

- Be prepared in a legible manner
- Include a description of the purpose of the trip
- Be summarized by traveler
- Identify the task order number
- Identify the task order CLIN
- Be submitted in advance of the travel with sufficient time to permit review and approval

All travel must be authorized by the COR and follow the task order and all other applicable requirements.

The contractor shall use only the minimum number of travelers and rental cars needed to accomplish the trip purpose. Travel shall be scheduled during normal duty hours whenever possible. Airfare will be reimbursed for actual common carrier fares which are obtained by the most reasonable and economical means.

The contractor shall provide a Trip Report for each trip associated with a travel approval. The contractor shall maintain a summary of all approved travel, to include at a minimum, the name of the traveler, location of travel, duration of trip, total cost of trip.

VIII. Government Furnished Materials, Facilities and Property

It is the expectations that all tasks can be performed offsite at the contractor's facility. CDC will provide any contractor personnel with a badge to access the CDC Roybal campus and the CDC network, as appropriate.

IX. Information Security and Privacy 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) employee 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. Protect 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:	[X] Low [] Moderate [] High
Availability:	[X] Low [] 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

4) **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 [] Moderate [] High

5) **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*.

6) **Protection of Sensitive Information**. For security purposes, information is *or* may be sensitive because it requires security to protect its confidentiality, integrity, and/or availability. The Contractor (and/or any subcontractor) sball protect 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 witb a FIPS 140-2 validated solution.

7) **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 and CDC policies. Unauthorized disclosure of information will be subject to the HHS/CDC 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).

8) **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).*

9) **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 always enable HTTP Strict Transport Security (HSTS) to instruct compliant browsers to assume HTTPS to reduce the number of insecure redirects and protect against attacks that attempt to downgrade connections to plain HTTP. For internal-facing websites, the HTTPS is not required, but it is highly recommended.

10) **Contract Documentation**. The Contractor shall use provided templates, policies, forms and other agency documents to comply with contract deliverables as appropriate.

11) **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 and CDC-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 (includiog 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 *[CDC-provided delivery date]*.

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. Encryptinn keys shall be provided to CDC Office of Chief Information Security Officer (OCISO).

12) **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 CDC 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.

13) **Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA)** – The Contractor shall assist the CDC Senior Official for Privacy (SOP) or designee with conducting a PTA for the information system and/or information handled under this contract in accordance with HHS policy and OMB M-03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.

a. The Contractor shall assist the CDC 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 CDC SOP that a review is required based on a major change to the system (e.g., new uses of information collected, changes to the way information is shared or disclosed and for what purpose, or when new types of PII are collected that could introduce new or increased privacy risks), whichever comes first.

B. 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/CDC 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 *CDC Security Awareness Training (SAT)* 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 (RBT) ***within 60 days*** of assuming their new responsibilities. Thereafter, they shall complete RBT at least ***annually*** in accordance with HHS policy and the *HHS Role-Based Training (RBT) of Personnel with Significant Security Responsibilities Memorandum*.

All HHS employees and contractors with SSR who ***have not*** completed the required training within the mandated timeframes shall have their user accounts disabled until they have met their RBT requirement.

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.

C. 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 *CDC 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.

D. Incident Response

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.
OMB Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information" (03 January 2017) states:

> **Definition of an Incident:**
> *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.*
> **Definition** of a **Breach:**
> *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.*

It further adds:

> A breach is not limited to an occurrence where a person other than an authorized user potentially accesses PU by means of a network intrusion, a targeted attack that exploits website vulnerabilities, or an attack executed through an email message or attachment. A breach may also include the loss or theft of physical documents that include PU and portable electronic storage media that store PU, the inadvertent disclosure of PU on a public website, or an oral disclosure of PII to a person who is not authorized to receive that information. It may also include an authorized user accessing PU for another 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".

Contracts with entities that collect, maintain, use, or operate Federal information or information systems on behalf of CDC shall include the following requirements:

1) The contractor shall cooperate with and exchange information with CDC officials, as deemed necessary by the CDC Breach Response Team, to report and manage a suspected or confirmed breach.

2) All contractors and subcontractors shall properly encrypt PII in accordance with OMB Circular A-130 and other applicable policies, including CDC-specific policies, and comply with HHS-specific policies for protecting PII. To this end, all contractors and subcontractors shall protect all sensitive information, including any PII created, stored, or transmitted in the performance of this contract to avoid a secondary sensitive information incident with FIPS 140-2 validated encryption.

3) All contractors and subcontractors shall participate in regular training on how to identify and report a breach.

4) All contractors and subcontractors shall report a suspected or confirmed breach in any medium as soon as possible and without unreasonable delay, consistent with applicable CDC IT acquisitions guidance, HHS/CDC and incident management policy, and United States Computer Emergency Readiness Team (US-CERT) notification guidelines. To this end, the Contractor (and/or any subcontractor) shall respond to all alerts/Indicators of Compromise (IOCs) provided by HHS Computer Security Incident Response Center (CSIRC) or CDC Computer Incident Response Team (CSIRT) within 24 hours via email at cdc@csirt.gov or telephone at 866-655-2245, whether the response is positive or negative.

5) All contractors and subcontractors shall be able to determine what Federal information was or could have been accessed and by whom, construct a timeline of user activity, determine methods and techniques used to access Federal information, and identify the initial attack vector.

6) All contractors and subcontractors shall allow for an inspection, investigation, forensic analysis, and any other action necessary to ensure compliance with HHS/CDC Policy and the HHS/CDC Breach Response Plan and to assist with responding to a breach.

7) Cloud service providers shall use guidance provided in the FedRAMP Incident Communications Procedures when deciding when to report directly to US-CERT first or notify CDC first.

8) Identify roles and responsibilities, in accordance with HHS/CDC Breach Response Policy and the HHS/CDC Breach Response Plan. To this end, the Contractor shall NOT notify affected individuals unless and until so instructed by the Contracting Officer or designated representative. If so, instructed by the Contracting Officer or representative, all notifications must be pre-approved by the appropriate CDC officials, consistent with HHS/CDC Breach Response Plan, and the Contractor shall then send CDC-approved notifications to affected individuals; and,

9) Acknowledge that CDC will not interpret report of a breach, by itself, as conclusive evidence that the contractor or its subcontractor failed to provide adequate safeguards for PII.

E. 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).

F. 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 by the effective date of this contract. Any revisions to the roster as a result of staffing changes shall be submitted immediately upon 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.

G. Contract Initiation and Expiration

1) **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).

2) **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.

3) **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.*

4) **Notification.** The Contractor (and/or any subcontractor) shall notify the CO and/or COR and system ISSO before an employee stops working under this contract.

5) **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 *CDC* policies.

6) The Contractor (and/or any subcontractor) shall perform and document the actions identified in the CDC Out-Processing Checklist (http://intranet.cdc.gov/od/hcrmo/pdfs/hr/Out_Processing_Checklist.pdf) when an employee terminates work under this contract. All documentation shall be made available to the CO and/or COR upon request.

H. 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 policies and shall not dispose of any records unless authorized by HHS.

If 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 policies.

Schedule of Deliverables

Deliverable Title/Description	Due Date
Roster	Before effective date of this contract
Contractor Employee Non-Disclosure Agreement (NDA)	Prior to performing any work on behalf of HHS
Assist in the completion of a PTA/PIA form	In conjunction with contract award
Copy of training records for all mandatory training	In conjunction with contract award and annually thereafter or upon request
Signed ROB for all employees	Initiation of contract and at least annually thereafter
Incident Report (as incidents or breaches occur)	As soon as possible and without reasonable delay and no later than 1 hour of discovery
Incident and Breach Response Plan	Upon request from government
List of Personnel with defined roles and responsibilities	Prior to performing any work on behalf of HHS

Deliverable Title/Description	Due Date
Off-boarding documentation, equipment and badge when leaving contract	At contract expiration after the Government's final acceptance of the work under this contract, or in the event of a termination of the contract.
Onboarding documentation when beginning contract.	Prior to performing any work on behalf of HHS
Form or deliverables required by CDC.	At contract expiration.

X. HHSAR Provision, 352.239-73: Electronic and Information Technology Accessibility Notice

By agreeing to the terms of the OADC Communication Services BPA, the offeror must comply with Section 508 standards for all deliverables in this task order. The offeror must complete an HHS/CDC checklist(s) as needed for each deliverable specified. The applicable Section 508 standards to this task order are: 1194.

205 WCAG 2.0 Level A & AA Success Criteria
302 Functional Performance Criteria
502 Inoperability with Assistive Technology
504 Authoring Tools
602 Support Documentation
603 Support Services

Performance Work Statement

I. Background and Need:

CDC's COVID-19 response activity works to ensure that all CDC audiences are provided with credible, timely and accurate information in order to prevent further spread of COVID-19. The Office of the Associate Director for Communication's (OADC) Digital Media Branch (DMB) is providing support for the Joint Information Center's (JIC) Social Media team supporting the COVID-19 response as well as supporting the primary CDC social media channels. Based on experience in managing social media in COVID-19, CDC seeks to update its social media best practices and review its efforts in order to modernize its social media activities. These social media communication modernization efforts will help CDC improve its social media content creation process, social media management, and social media guidance for use during large scale emergencies and day-to-day digital content needs of the agency.

II. Project Objective:

The objective of this task order is to secure social media services for supporting modernization of CDC's social media efforts. This work will also tie into a broader digital communication modernization effort being carried out in DMB. The focus of this work is to develop products that will assist CDC in advancing and improving its social media efforts.

Ultimately, this work will ensure that CDC's social media audiences will receive optimized and relevant social media health messages.

III. Description of Work

The contractor shall support CDC in the development of social media modernization recommendations, social media strategy, guidance and trainings and support for managing areas of social media misinformation.

Task 1. Project Management

a. Kickoff Meeting - A kickoff meeting shall be held no later than 10 work days after the initial award is made to discuss plans and timelines as well as clarify roles and responsibilities, to be held remotely.
b. Work Plan - Following the kickoff meeting, the contractor shall develop and write a short work plan, including all essential interim and final deliverables, key staff responsible for tasks (ineluding contractors, CDC staff, or other partners), and schedule of key deadlines (including review cycles and absolute No Later Than (NLT) dates for key activities and deliverables) for COR review and correction before acceptance. The work plan must contain:
    a. A list confirming the reports and activities proposed by the contractor and a schedule for the project plans described below.
    b. Contractor plan for employee management including how the contractor shall avoid any appearances of personal services by CDC.
    c. Schedule for Estimate at Complete (EACs)
    d. Plan to ensure accuracy of all ads posted and assurance all content has been cleared and approved.

The work plan is due no later than 10 work days following the kickoff meeting. The work plan (and any schedule of interim deliverables) may be revised according to CDC acceptance of the updated work plan by the COR during the project with the restriction that these changes must not impact the overall period of performance, scope, or specifications of the award, or otherwise impinge on the authority of the contracting officer. It is the responsibility of the contractor to fully understand what changes require contracting officer approval.

c. Quarterly Conference Call – A quarterly conference call with CDC COR must be held. The meeting shall be initiated and led by the contractor. The purpose of this call is ongoing review of task performance. The discussion from the conference call must be documented via e-mail after the meeting. Any required performance improvements must be documented/reported via e-mail to the COR after the meeting.

Task 2. Identify areas of modernization in CDC's social media efforts in emergency and non-emergency situations.

The vendor shall provide recommendations to CDC in modernizing CDC's social media efforts.

To inform these recommendations, the vendor shall consider industry best practices and techniques for using social media to communicate health information. The vendor shall perform a high-level review of CDC's social media efforts during the COVID-19 response. The vendor shall also perform a high-level review of CDC's current process of supporting non-emergency social media. DMB can provide historical information on processes, metrics, efforts, templates, and other artifacts related to our efforts. The vendor shall also review other health content providers for best practices and techniques relevant to CDC's effort.

The vendor shall identify areas that CDC can improve, streamline, and modernize CDC's overall social media efforts. The vendor shall address social media in non-emergency and emergency areas. The vendor shall proactively identify areas to explore, but it is anticipated that the following areas must be addressed:

a) Avenues to speed up social media development in CDC's existing content process
b) New ways to use video, live events, and other motion graphics quickly and effectively
c) Social media monitoring improvements particularly during emergencies
d) Content quality, consistency, format and design
e) Content optimization and tracking
f) New tactics and strategies to leverage social media channels
g) Comment moderation
h) Enhancing engagement

The vendor shall specifically address ways CDC should incorporate new efforts, activities, tools and techniques. The vendor shall provide recommendations that can be explored with existing staff and tools as well as efforts that may require new tools or staff. If new tools are needed, the vendor shall provide recommendations and/or recommended tool requirements. As well, new staff or skill recommendations shall also be provided, if that is a vendor recommendation.

The contractor shall:

a. Develop and submit for CDC's approval, a project plan for the work described in Task 2. The plan shall be developed in consultation with OADC's social media team. The project plan shall include an outline of the project's objectives, tactics, areas to be explored, and a timeline.
b. Deliver a modernization recommendation report. The vendor shall deliver a draft report of findings and recommendations for modernization within 4 months of award. The vendor shall then deliver a final report within 6 months of award. This final report shall address CDC comments on the draft report. The report shall include an analysis of the current state of social media at CDC, any lessons learned from COVID-19, identification of current problems, identification of areas that work well, all modernization recommendations including recommended next steps, needed tools, process changes and other information relevant to the vendor's recommendations.
c. Within 2 weeks of report finalization (Task 3, b), the vendor shall develop a presentation (PowerPoint) to communicate the report findings and recommendations to groups at CDC including the JIC, CDC Social Media Council and Associate Directors of Communication (ADCS). The vendor shall deliver a draft slide deck for comment and review and a final deck incorporating feedback. The slide deck shall incorporate plain language, visuals to illustrate findings, and talking points.

Task 3. Develop a CDC social media strategy

Based on efforts in Tasks 2, the vendor shall develop a CDC social media strategy. The strategy shall reflect best practices for social media content strategies and modernization recommendations from Task 2. The strategy shall reflect a strong expertise in social media strategies. The strategy shall also consider digital first principles. The strategy shall leverage best practices for large distributed organizations such as CDC. Given the wide variety of topics supported at CDC, the strategy shall focus on elements that can apply to all of CDC's social media activities and include guiding principles, tacties, goals, etc.

The contractor shall:

a. Deliver a draft social media strategy within 4.5 months of award.
b. After the draft has been developed that DMB approves, the vendor shall assist in soliciting input from across CDC including CDC's Social Media Council, ADCS, JIC staff, and health communication specialists. Engagement with these groups must be through e-mails as well as 2-3 presentations to the groups, as needed. The vendor shall review comments, input and suggestions for incorporation or response.
c. Deliver a final strategy within 7.5 months of award.
d. Within 2 weeks of report finalization (Task 2, b), the vendor shall develop a presentation to describe the strategy to groups at CDC including the JIC, CDC Social Media Council and Associate Directors of Communication (ADCS). The vendor shall deliver a draft slide deck for comment and review and a final deck incorporating feedback.

Task 4. Support for CDC's Social Media Guidance, Policies, and Training

Based on work in Task 2-3, the vendor shall assist CDC in updating its existing social media guidance materials and develop new needed social media guidelines, policies and training materials. The vendor shall incorporate current industry best practices, specifications and standards. The contractor shall update

these existing materials, develop new identified materials, and recommend other materials based on work developed in this task order.

a. The vendor shall submit a project plan for this task with a suggested list of documents for updating or new development, along with a proposed timeline to the COR and social media lead for approval.
b. The vendor shall update or create an estimated 15-20 documents or guides. For each document, the vendor shall also draft a proposed outline for materials for approval prior to full content development. The vendor shall submit a draft to CDC and allow 2-4 weeks for CDC comment. The vendor's final version shall address comments and suggestions.

   It is anticipated that the below documents shall be updated or created, as part of the 15-20 document delivered for this task. However, the final list must be determined in the project plan developed in Task 4a.

   1. Recommend updates to CDC's social media policy (CDC Enterprise Social Media Policy)
   2. Plain language version of CDC's social media policy
   3. Updates and development of a Social Media Best Practices & Style Guide document for each CDC channel including Instagram, Facebook, LinkedIn, Twitter, and Pinterest. (Examples located at: CDC Social Media Tools, Guidelines & Best Practices | Social Media | CDC)
      a. These materials shall include items such as sizing parameters, character limits, audience recommendations, writing styles for each channel, best practices, comment moderation, and ways to best optimize content on these channels.
   4. Develop a new social media SOP for emergency response to include process, comment monitoring, and all aspects of managing social media during an emergency.
   5. Develop style guide for emergency response (ER) content that outlines ways ER content should differ or stand out from standard content. For example, should use of terms such as "ALERT" be used in ER content and associated graphics.
   6. Develop a new guide on how to use and administer social media ads. The guide shall address all platforms including, but not limited to Facebook, Twitter, Instagram, Snapchat, YouTube, Pinterest, WhatsApp and others as the need arises.
   7. Develop a COVID-19 Social Media Retrospective presentation. This presentation shall include an overview of general social media activities performed during COVID-19, most effective social media wins, partnerships, problems, and lessons learned for use at CDC meetings with ADCS, Social Media Council and other communicators. Efforts in task 2-3 will likely inform this effort. JIC social media team can provide suggestions.
   8. Develop a new intranet-based set of FAQs for CDC social media managers based on most common questions asked by social media managers at CDC. A list of questions will be provided to the vendor. Answers must be based on work throughout this task order.
   9. Evaluate if an update to CDC's Writing for Social media is needed and if so, update the document or incorporate into channels specific guidance (See: Guide to Writing for Social Media | Social Media | CDC)

The vendor shall develop slide based trainings for up to 7 social media topic areas identified through the work on the contract. The contractor does not need to deliver the training only create the slide deck.

Task 6. Support Social Media Team in Addressing Misinformation

Provide support to OADC's social media team on misinformation monitoring and reporting efforts. The contractor shall work closely with the OADC misinformation team comprised of the social media team, OADC's risk communication experts, and a misinformation monitoring and reporting team supported via IAA with CDC and the U.S. Census. This team has a system already available to provide misinformation reports that include an analysis of rumors, misinformation, disinformation, trends and behavior including number of unique and organic shares and blue check mark engagement. These reports also include specific recommendations on misinformation to act on.

The vendor shall:

a. Participate in misinformation review meetings 1-3 times per week. Track action items from the meeting. Lead CDCs preparation for these meetings including suggesting agenda items, bring up issues or problems or follow-up.
b. Assist in review of weekly misinformation reports provided by the OADC team. The vendor shall assist in identifying actionable content and will research the issue on CDC.gov or other social media assets. The vendor shall then develop content that can be shared with fact-checkers or social media platforms regarding the facts related to areas of misinformation. It is expected that on average, the vendor shall work with 1-4 items of misinformation per week.
c. The vendor shall help track, via a spreadsheet or other tools, specific areas of misinformation and ensure that responses have been cleared, the issues have been reported and all follow up is complete. The vendor shall assist the team in maintaining full records of all actions.
d. The vendor shall participate in social media team meetings 1 time per week to ensure the OADC social media team and JIC social media team are aware of misinformation needs and assist, as needed, in developing comment responses and/or social media to post on CDC channels.
e. Assist in developing slides or other communication materials to educate and communicate this effort to the Social Media Council 2-4 times per year.

It is the expectation that this work in Task 5 is roughly 10-20 hours a week and must enhance the connection between the misinformation team and OADC's social media efforts.

IV. Deliverables:

All task order deliverables intended for communication to the public must comply with Public Law 111–274, the Plain Writing Act of 2010. For Plain Language information and the Federal Plain Language Guidelines see www.plainlanguage.gov.

Task No	Deliverable	Quantity	Delivery Method	Deliver To	Due Date
1	Task 1: Kickoff Meeting	1 (per year)	Electronically via E-mail	COR and DMB Social Media Leads	10 working days following award
2	Task 1: Work Plan	1 (per year)	Electronically via E-mail	COR and DMB Social Media Lead	20 working days following kickoff meeting
3	Task 1: Quarterly Conference Call	4 (per year)	Electronically via E-mail	COR and DMB Social Media Lead	Within the last 4 weeks of the end of each quarter

4	Task 2: Project Plan	1	Electronically via E-mail	COR and DMB Social Media Lead	First draft due 30 days after award.
5	Task 2: Modernization Report	2 (1 final, 1 draft)	Electronically via E-mail	COR and DMB Social Media Lead	Draft due 3.5 months after award, Final due 5.5 months after award.
6	Task 2: Presentation of Findings	1	n/a	COR and DMB Social Media Lead	2 weeks after modernization report finalization.
7	Task 3: Project Plan	1	Electronically via E-mail	COR and DMB Social Media Lead	First draft due 30 days after award.
8	Task 3: Social Media Strategy	2 (1 final, 1 draft)	Electronically via E-mail	COR and DMB Social Media Lead	Draft due 4.5 months after award, Final due 7.5 months after award.
9	Task 3: Presentation of Findings	1	Electronically via E-mail	COR and DMB Social Media Lead	2 weeks after strategy finalization.
10	Task 4: Project plan	1	Electronically via E-mail	COR and DMB Social Media Lead	Due 4 months after award. The plan can be adjusted as need change. Vendor and COR can agree to adjustments.
11	Task 4: Updates to CDC social Media Guidance and documents	15-20	Electronically via E-mail	COR, DMB Social Media Lead & Social media staff POCs assigned based on topic of document.	Timeline based on project plan agreed on by CDC. All documents completed by end of award. It is expected work on these documents would be spread out through the life of the contract.
12	Task 4: Social media Slides	7 decks	Electronically via E-mail	COR and DMB Social Media Lead	All decks completed 11 months after award.
13	Task 5: Misinformation	1-4 misinformation facts/recommendations	Electronically via E-mail	COR and OADC Misinformation lead	Weekly
14	Task 5: Misinformation Presentations	2-4 slide decks	Electronically via E-mail	COR and OADC Misinformation lead	2-4 times over life of task order

All materials must be submitted electronically in MS compatible format that meets CDC standards and is readily available at CDC (e.g. MS Office [Word, Excel, PowerPoint]) or Adobe Acrobat. All reporting requirements and written deliverables as part of this contract must be supplied to the project Contracting Officer Representative (COR). Acceptance of any written deliverables is pending CDC COR review and correction to any resulting comments, to be confirmed in writing and documented via e-mail to the COR. Any schedule of interim deliverables may be revised according to CDC acceptance of an updated written work plan by the COR during the project with the restriction that these changes must not impact the overall period of performance, scope, or specifications of the award, or otherwise impinge on the

authority of the contracting officer. It is the responsibility of the contractor to fully understand what changes require contracting officer approval.

V. Performance Matrix:

Work Requirement	Acceptable Quality Level (AQL)	Monitoring Method	Incentives/ Disincentives
Task 1 Kick off meeting (base year and repeated annually)	• Occurs at regularly scheduled times • Contractor is prepared to discuss relevant project issues, is responsive to project planning issues/project improvments, and documents meetings as described in PWS (may be corrected to COR comments)	• 100% review of event (by the COR) • Unacceptable meetings will be documented as customer complaints, contractor may be allowed to correct any insufficiences to CDC satisfaction	• Contractor's performance is documented as past performance using CPARS which is considered for future awards. • Performance is considered in determining whether to exercise the option periods • Repeated complaints on different events/tasks but the same issue will be elevated for higher level resolution (senior management and/or OAS)
Task 1 Work Plan	• Appropriate content is included as outlined in the PWS • Appropriate content is included as outlined in the PWS (may be corrected to COR comments)	• 100% review of delivered reports (by the COR) • Unacceptable quarterly conference meetings will be documented as customer complaints, contractor may be allowed to correct any insufficiences to CDC satisfaction	
Task 1 Quarterly Conference Calls	• Occurs at regularly scheduled times (100% within schedule) • Contractor is prepared to discuss relevant work performance, is responsive to performance issues, and documents quarterly meetings as described in PWS	• 100% review of events (by the COR) • Unacceptable quarterly conference meetings will be documented as customer complaints, contractor may be allowed to correct any insufficiences to CDC satisfaction	
Task 2: Social Media Modernization Report	• Plans are delivered on time 90% • Report provides relevant recommendations and technical details • Report reflect understanding of CDC's business requirments • Reports scope out realistic timelines • Reports refelect research into industry best practices	• 100% review of strategy (by the COR and social media lead)	
Task 4: Guidance updates	• Documents are error free 90% time. • Documents provide relevant best pratices and technical details • Documents reflect understanding of CDC's processes and channel specificiations.	• 100% review of documents (by the social media team)	

Work Requirement	Acceptable Quality Level (AQL)	Monitoring Method	Incentives/ Disincentives
Task 5: Misinformation	• Tasks are completed weekly and reflect strong understanding of social media, misinformation • Tasks are accurately tracked on spreadsheet	• 100% of recommendations (by the DMB or OADC staff) • Unacceptable recommendations or fact checking shall be reported to project manager • Review of tasks on spreadsheet during weekly meetings	

VI. Period of Performance:

The period of performance is:

Year 1 (Basic Period): 9/1/2021-8/31/2022

VII. Place of Performance:

Work shall be performed at the contractor's facilities. Work can be remote to Atlanta.

VIII. Government Furnished Materials, Facilities and Property

CDC will provide network access and equipment for contract staff administering ads.

IX. HHSAR Provision, 352.239-73: Electronic and Information Technology Accessibility Notice
Electronic and Information Technology Accessibility

(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 when Federal agencies develop, procure, maintain, or use electronic and information technology, Federal employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who are not individuals with disabilities, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency.

(b) Accordingly, any offeror responding to this solicitation must comply with established HHS EIT accessibility standards. Information about Section 508 is available at http://www.hhs.gov/web/508. The complete text of the 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 contract are: 1194.
205 WCAG 2.0 Level A & AA Success Criteria
302 Functional Performance Criteria
502 Inoperability with Assistive Technology
504 Authoring Tools
602 Support Documentation
603 Support Services

In order to facilitate the Government's determination whether proposed EIT supplies meet applicable Section 508 accessibility standards, offerors must submit an HHS Section 508 Product Assessment Template, in accordance with its completion instructions. The purpose of the template is to assist HHS acquisition and program officials in determining whether proposed EIT supplies conform to applicable Section 508 accessibility standards. The template allows offerors or developers to self-evaluate their supplies and documentation detail - whether they conform to a specific Section 508 accessibility standard, and any underway remediation efforts addressing conformance issues. Instructions for preparing the HHS Section 508 Evaluation Template are available under Section 508 policy on the HHS Web site http://hhs.gov/web/508.

In order to facilitate the Government's determination whether proposed EIT services meet applicable Section 508 accessibility standards, offerors must provide enough information to assist the Government in determining that the EIT services conform to Section 508 accessibility standards, including any underway remediation efforts addressing conformance issues.

(d) Respondents to this solicitation must identify any exception to Section 508 requirements. If a offeror claims its supplies or services meet applicable Section 508 accessibility standards, and it is later determined by the Government, i.e., after award of a contract or order, that supplies or services delivered do not conform to the accessibility standards, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its expense.

(e) Electronic content must be accessible to HHS acceptance criteria. Checklist for various formats are available at http://508.hhs.gov/, or from the Section 508 Coordinator listed at https://www.hhs.gov/web/section-508/additional-resources/section-508-contacts/index.html. Materials that are final items for delivery should be accompanied by the appropriate checklist, except upon approval of the Contracting Officer or Representative.

(End of provision)

Statement of Work

Title: Media Buy Next Door Ads

SECTION 1 – BACKGROUND

The Centers for Disease Control and Prevention (CDC), National Center for Emerging and Zoonotic Infectious Diseases (NCEZID) aims to prevent disease, disability, and death caused by a wide range of infectious diseases. NCEZID focuses on diseases that have been around for many years, emerging diseases (those that are new or just recently identified), and zoonotic diseases (those spread from animals to people). NCEZID's work is guided in part by a holistic "One Health" strategy, which recognizes the vital interconnectedness of microbes and the environment. Through a comprehensive approach involving many scientific disciplines, we can attain better health for humans and animals and improve our environment.
To carry out our mission, NCEZID uses many different tactics: providing leadership in public health, conducting exemplary science, strengthening preparedness efforts, establishing public health policy, sharing vital health information with the public, and building partnerships. Each of the center's seven divisions works with partners to protect and improve the public's health in the United States and worldwide.
This project supports the Division of Vector-Borne Diseases (DVBD). To achieve their mission to reduce illness and death due to vector-borne diseases, DVBD has identified the following goals:
Goal 1: Identify and detect vector-borne pathogens that cause disease in people.
Goal 2: Understand when, where, how often, and how people are exposed to vector-borne pathogens.
Goal 3: Prevent exposure to vector-borne pathogens and mitigate consequences of infection.
Goal 4: Implement vector-borne disease diagnostics, surveillance, control and prevention programs developed in goals 1 through 3.

SUBSECTION A – DEFINITIONS
N/A

SECTION 2 – PURPOSE

The purpose of this contract is to procure media ads to be placed on Nextdoor, an online community platform meant to bring neighbors together to share information, goods, and services.
According to Pew Research seven out of ten Americans use social media to connect with peers, engage with news content, share information, and entertain themselves. Public health has long capitalized on the use of digital advertising to reach consumers where they are. Depending on your audience, message, and campaign goals there are numerous digital platforms that may be used to target at risk populations.
For the purpose of mosquito-borne diseases, geographic location is often the factor most closely tied to risk. For this reason, the Arboviral Diseases Branch (ADB) is proposing to use the digital platform Nextdoor to geotarget consumers in high-risk areas with important mosquito-bite prevention messages.
In order to sign up for Nextdoor, you must provide your current address so that you can be added to your location's neighborhood group. Neighbors within a Nextdoor community can post about local information they've heard, lost pets, free curbside items, and any number of other community related topics.
Many local mosquito control organizations already use Nextdoor to share information about spraying events or confirmed disease cases. Nextdoor allows businesses to join and specify geographic locations, based on zip code, where they would like their posts displayed.
The Nextdoor platform is ideal for sharing health information for specific geographic targets. Nextdoor users are invested in their community and are actively seeking information whenever they log in. Users are likely to read and engage with health messages posted within their feed. During an outbreak The

purpose of this purchase is to have the ability to target messages to just the neighborhoods that are highly impacted by arbovirus disease affected. This more precise approach would also help support State and local health departments who may not have the resources to or bandwidth for additional message targeting during an outbreak.

SECTION 3 – SCOPE OF WORK

The Contractor shall purchase ads to be placed on Nextdoor during specified timelines outlined in the deliverables table below. The purpose is to support local communication efforts during a mosquito-borne disease outbreak or heightened diseases activity. Messages will be placed on Nextdoor and geotargeted to communities most at risk to encourage them to take preventative measures to avoid mosquito bites.
The Vendor shall manage media placement on the Nextdoor platform as requested by CDC. Placement and timeline will be decided based on disease activity which typically peaks between July and October.
CDC will provide creative content for placement.
The Vendor will provide weekly reports of ad performance via email and adjust ad placements as necessary depending on ad performance. A final summary of ad performance will be provided to CDC following completion of the ad placements.

SECTION 4 – TASKS TO BE PERFORMED

4.1 NCEZID, DVBD, ADB Media Buy NextDoor

4.1.1 Vendor shall manage all aspects of media purchase and placement on the Nextdoor platform as requested by CDC. Labor would include approximately 20 hours per contract period.

4.1.2 Vendor shall communicate verbally and in writing with CDC staff to determine targeting and timeline for ad placement.

4.1.3 CDC will provide creative content for all ad placement.

4.1.4 The Vendor will share Nextdoor automated weekly reports of ad performance via email and if needed, adjust ad placements as directed by CDC.

4.1.5 Vendor shall provide the NextDoor automatically generated summary of ad performance to CDC following completion of the ad placements.

SECTION 5 – GOVERNMENT FURNISHED MATERIALS

The Government will provide media content for ads.

SECTION 6 – PERIOD OF PERFORMANCE

The period of performance shall be a base period of 12 months beginning 9/20/2021 with an option period from 9/20/2022 to 9/19/2023.

SECTION 7 – PLACE OF PERFORMANCE

Vendor location

SECTION 8 – DELIVERABLES/REPORTING SCHEDULE

Task Order Deliverables and Milestones

Item #	Description	Quantity or Number of Copies	Delivery Date	Deliver to
1	Media purchase and placement on the Nextdoor platform as requested by CDC. (task 4.1.1 above)	N/A	July through October	COR
2	Communicate verbally and in writing with CDC staff to have kick off call determine targeting and timeline for ad placement. (relates to Task 4.1.2 above)	N/A	Up to four conference calls per period of performance and email communication ad hoc during period of performance	COR
3	CDC will provide all creative content for all ads (relates to Tasks 4.1.3 above)	N/A	One time delivery during period of performance	COR
4	The Vendor will provide weekly reports of ad performance via email and adjust ad placements. (relates to Tasks 4.1.4 above)	N/A	Occurs weekly during during ad buy	COR
5	Vendor shall provide an automatically generated summary of ad performance from NextDoor to CDC following completion of the ad placements (relates to Task 4.1.5 above)	N/A	Occurs at the completion of ad placement	COR

SECTION 9 – TRAVEL

N/A

SECTION 10 – PAYMENT TERMS

This contract is a fixed price contract.

SECTION 11 – REFERENCE MATERIALS

N/A

SECTION 12 – CONTRACTING OFFICER'S REPRESENTATIVE INFORMATION

The Contracting Officer's Representative (COR) for this procurement is:
Tracy Hasvold
Centers for Disease Control and Prevention
Division of Vector Borne Diseases
3156 Rampart Road
Fort Collins, Colorado 80521

Telephone Number: 970-221-6422
E-mail Address:tab7@cdc.gov
Preferred method of communication: E-mail

1.1 **SECTION 13** – 508 of the Rehabilitation Act

SECTION 13 – HHSAR Provision, 352.239-73: Electronic and Information Technology Accessibility Notice
(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 when Federal agencies develop, procure, maintain, or use electronic and information technology, Federal employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who are not individuals with disabilities, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency.

(b) Accordingly, any offeror responding to this solicitation must comply with established HHS EIT accessibility standards. Information about Section 508 is available at http://www.hhs.gov/web/508. The complete text of the 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 contract are: 1194.
205 WCAG 2.0 Level A & AA Success Criteria
302 Functional Performance Criteria
502 Inoperability with Assistive Technology
504 Authoring Tools
602 Support Documentation
603 Support Services

In order to facilitate the Government's determination whether proposed EIT supplies meet applicable Section 508 accessibility standards, offerors must submit an HHS Section 508 Product Assessment Template, in accordance with its completion instructions. The purpose of the template is to assist HHS acquisition and program officials in determining whether proposed EIT supplies conform to applicable Section 508 accessibility standards. The template allows offerors or developers to self-evaluate their supplies and documentation detail - whether they conform to a specific Section 508 accessibility standard, and any underway remediation efforts addressing conformance issues. Instructions for preparing the HHS Section 508 Evaluation Template are available under Section 508 policy on the HHS Web site http://hhs.gov/web/508.

In order to facilitate the Government's determination whether proposed EIT services meet applicable Section 508 accessibility standards, offerors must provide enough information to assist the Government in determining that the EIT services conform to Section 508 accessibility standards, including any underway remediation efforts addressing conformance issues.

(d) Respondents to this solicitation must identify any exception to Section 508 requirements. If a offeror claims its supplies or services meet applicable Section 508 accessibility standards, and it is later determined by the Government, i.e., after award of a contract or order, that supplies or services delivered do not conform to the accessibility standards, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its expense.

(End of provision)

1.2 Non-Disclosure Agreement for Contractor and Contractor Employees (May 2009)

A. The contractor shall prepare and submit a Non-Disclosure Agreement (NDA) to the Contracting Officer prior to access of government information or the commencement of work at CDC.

B. The NDA made part of this clause, exhibit I and II, is required in service contracts where positions and/or functions proposed to be filled by contractor's employees will have access to non-public and procurement-sensitive information. The NDA also requires contractor's employees properly identify themselves as employees of a contractor when communicating or interacting with CDC employees, employees of other governmental entities (when communication or interaction relates to the contractor's work with the CDC), and members of the public. The Federal Acquisition Regulation (FAR) 37.114 (c), states "All contractor personnel attending meetings, answering Government telephones, and working in other situations where their contractor status is not obvious to third parties are required to identify themselves as such to avoid creating an impression in the minds of members of the public or Congress that they are Government officials, unless, in the judgment of the agency, no harm can come from failing to identify themselves. They must also ensure that all documents or reports produced by contractors are suitably marked as contractor products or that contractor participation is appropriately disclosed."

C. The Contractor shall inform employees of the identification requirements by which they must abide and monitor employee compliance with the identification requirements.

D. During the contract performance period, the Contractor is responsible to ensure that all additional or replacement contractors' employees sign a NDA and it is submitted to the Contracting Officer prior to commencement of their work with the CDC.

E. Contractor employees in designated positions or functions that have not signed the appropriate NDA shall not have access to any non-public, procurement sensitive information or participate in government meeting where sensitive information may be discussed.

F. The Contractor shall prepare and maintain a current list of employees working under NDA's and submit to the Contracting Officer upon request during the contract period of performance. The list should at a minimum include: contract number, employee's name, position, date of hire and NDA requirement. (End of Clause)

1.3 Prohibition of Food, Meals and Light Refreshments

The inclusion of food, meals, beverages or light refreshments is expressly prohibited in the performance of this contract and is considered an unallowable contract expense. This prohibition on the inclusion of food will be flowed down and included in all subcontracts, purchase orders, and agreements issued in the performance of this contract. Food and meals may not be accepted and will not be provided even if offered at no additional cost to CDC.
(End of Clause)

The below information complies with CDC Security and Privacy compliance requirements for E-Government Act of 2002 (FISMA 2002) and Federal Information Security Modernization Act of 2014 (FISMA 2014)

Security Compliance

- If the contractor will host or create an information system on behalf of the CDC, provide IT services to the CDC, or provide IT products to the CDC, then the contractor shall comply with the applicable IT security references below (Standards 1 - 4).

Standard-1: Procurements Requiring Information Security and/or Physical Access Security

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) employee 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. Protect 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:	[x] Low [ ] Moderate [ ] High
Integrity:	[x] Low [ ] Moderate [ ] High
Availability:	[x] Low [ ] Moderate [ ] High
Overall Risk Level:	[x] Low [ ] 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 (Non Sensistive Internal User name and id)

Complete this section using the information obtained from the Security and Privacy Checklist in Appendix A, parts A and B.

4) **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: [x] Low [ ] Moderate [ ] High

5) **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 32 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*.

6) **Protection of Sensitive Information**. For security purposes, information is *or* may be sensitive because it requires security to protect its confidentiality, integrity, and/or availability. The Contractor (and/or any subcontractor) shall protect 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.

7) **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 and *[CDC]* policies. Unauthorized disclosure of information will be subject to the HHS/*[CDC]* 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).

8) **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)*. .

9) **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 protect against attacks that attempt to downgrade connections to plain HTTP. For internal-facing websites, the HTTPS is not required, but it is highly recommended.

10) **Contract Documentation**. The Contractor shall use provided templates, policies, forms and other agency documents to comply with contract deliverables as appropriate.

See Appendix D *for baseline deliverables.*

11) **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 and CDC-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 CDC Office of Chief Information Security Officer (OCISO).

12) **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 CDC 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.

See Appendix C *for the Contractor Non-Disclosure Agreement.*

13) **Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA)** – The Contractor shall assist the CDC Senior Official for Privacy (SOP) or designee with conducting a PTA for the information system and/or information handled under this contract in accordance with HHS policy and OMB M-03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.
    a. The Contractor shall assist the CDC 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 CDC SOP that a review is required based on a major change to the system (e.g., new uses of information collected, changes to the way information is shared or disclosed and for what purpose, or when new types of PII are collected that could introduce new or increased privacy risks), whichever comes first.

A. 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/CDC 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 *CDC Security Awareness Training (SAT), 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 (RBT) ***within 60 days*** of assuming their new responsibilities. Thereafter, they shall complete RBT at least ***annually*** in accordance with HHS policy and the *HHS Role-Based*

Training (RBT) of Personnel with Significant Security Responsibilities Memorandum.
All HHS employees and contractors with SSR who ***have not*** completed the required training within the mandated timeframes shall have their user accounts disabled until they have met their RBT requirement.

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.

B. 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 *CDC 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.

C. Incident Response

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.

OMB Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information" (03 January 2017) states:

Definition of an Incident:

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.

Definition of a **Breach:**

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.

It further adds:

A breach is not limited to an occurrence where a person other than an authorized user potentially accesses PII by means of a network intrusion, a targeted attack that exploits website

vulnerabilities, or an attack executed through an email message or attachment. A breach may also include the loss or theft of physical documents that include PII and portable electronic storage media that store PII, the inadvertent disclosure of PII on a public website, or an oral disclosure of PII to a person who is not authorized to receive that information. It may also include an authorized user accessing PII 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".

Contracts with entities that collect, maintain, use, or operate Federal information or information systems on behalf of CDC shall include the following requirements:

1) The contractor shall cooperate with and exchange information with CDC officials, as deemed necessary by the CDC Breach Response Team, to report and manage a suspected or confirmed breach.
2) All contractors and subcontractors shall properly encrypt PII in accordance with OMB Circular A-130 and other applicable policies, including CDC-specific policies, and comply with HHS-specific policies for protecting PII. To this end, all contractors and subcontractors shall protect 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.
3) All contractors and subcontractors shall participate in regular training on how to identify and report a breach.
4) All contractors and subcontractors shall report a suspected or confirmed breach in any medium as soon as possible and no later than 1 hour of discovery, consistent with applicable CDC IT acquisitions guidance, HHS/CDC and incident management policy, and United States Computer Emergency Readiness Team (US-CERT) notification guidelines. To this end, the Contractor (and/or any subcontractor) shall respond to all alerts/Indicators of Compromise (IOCs) provided by HHS Computer Security Incident Response Center (CSIRC) or CDC Computer Incident Response Team (CSIRT) within 24 hours via email at csirt@cdc.gov or telephone at 866-655-2245, whether the response is positive or negative.
5) All contractors and subcontractors shall be able to determine what Federal information was or could have been accessed and by whom, construct a timeline of user activity, determine methods and techniques used to access Federal information, and identify the initial attack vector.
6) All contractors and subcontractors shall allow for an inspection, investigation, forensic analysis, and any other action necessary to ensure compliance with HHS/CDC Policy and the HHS/CDC Breach Response Plan and to assist with responding to a breach.
7) Cloud service providers shall use guidance provided in the FedRAMP Incident Communications Procedures when deciding when to report directly to US-CERT first or notify CDC first.
8) Identify roles and responsibilities, in accordance with HHS/CDC Breach Response Policy and the HHS/CDC Breach Response Plan. To this end, the Contractor shall NOT notify affected individuals unless and until so instructed by the Contracting Officer or designated representative. If so instructed by the Contracting Officer or representative, all notifications must be pre-approved by the appropriate CDC officials, consistent with HHS/CDC Breach Response Plan, and the Contractor shall then send CDC- approved notifications to affected individuals; and,
9) Acknowledge that CDC will not interpret report of a breach, by itself, as conclusive evidence that the contractor or its subcontractor failed to provide adequate safeguards for PII.

D. Position Sensitivity Designations

All Contraetor (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 requiring activity representative, in conjunction with Personnel Security, shall use the OPM Position Sensitivity Designation automated tool (https://www.opm.gov/investigations/) to determine the sensitivity designation for background investigations. After making those determinations, include all applicable position sensitivity designations.

E. 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.*

For additional information, see HSPD-12 policy at: https://www.dhs.gov/homeland-security-presidential-directive-12)

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 by the effective date of this contract. Any revisions to the roster as a result of staffing changes shall be submitted immediately upon 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.

F. Contract Initiation and Expiration

1) **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
CDC EPC Requirements: https://www2a.CDC.gov/CDCup/library/other/eplc.htm

2) **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.
3) **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*.

4) **Notification.** The Contractor (and/or any subcontractor) shall notify the CO and/or COR and system ISSO before an employee stops working under this contract.
5) **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 *CDC* policies.
6) The Contractor (and/or any subcontractor) shall perform and document the actions identified in the CDC Out-Processing Checklist (http://intranet.cdc.gov/od/hcrmo/pdfs/hr/Out_Processing_Checklist.pdf) when an employee terminates work under this contract. All documentation shall be made available to the CO and/or COR upon request.

G. 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 policies and shall not dispose of any records unless authorized by HHS.

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 policies.

Standard-2: Requirements for Procurements Involving Privacy Act Records

Appropriate security controls and Rules of Behavior should be incorporated to protect the confidentiality of information, proprietary, sensitive, and Personally Identifiable Information (PII) the Contractor may come in contact with during the performance of this contract. Contractor will only have access to Active Directory User Name and User ID, there will be no access to user password.

Standard-3: Procurements Involving Government Information Processed on GOCO or COCO Systems

A. Security Requirements for GOCO and COCO Resources

1) **Federal Policies.** The Contractor (and/or any subcontractor) shall comply with applicable federal directives that include, but are not limited to, the *HHS Information Security and Privacy Policy (IS2P)*, the *CDC Protection of Information Resources* policy; *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 protect 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 prior to any use of the system in a production capacity, i.e., its intended users able to collect, store, process or transmit data to fulfill the system's function. The Contractor shall

conduct the SA&A requirements in accordance with *HHS IS2P/ CDC Protection of Information Resources*; the *CDC IT Security Program Implementation Standards;* the *CDC Security Assessment and Authorization (SA&A) Standard Operating Procedure;* and NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (latest revision).

CDC 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 to the C/I/O Information System Security Officer (ISSO) in accordance with the timeline, process and formats proscribed for a Full system authorization in the CDC Security Assessment and Authorization Standard Operating Procedure (CDC SA&A SOP). The following SA&A deliverables are required to complete the SA&A package:

- **Baseline System Information (BSI)** – The Contractor will document a system overview, in accordance with the timeline, process and formats described in the *CDC SA&A SOP*. The BSI will include information concerning: system identification and ownership; system data, information types, impact levels and system categorization; system functional description / general purpose; system authorization boundary and environment; system user descriptions; and system interconnections and dependencies. The Contractor shall update the BSI at least ***annually*** thereafter.
- **Privacy Threshold Analysis / Privacy Impact Analysis** – The Contractor (and/or any subcontractor) shall provide a PTA/PIA (as appropriate), in accordance with the timeline, process and formats described in the *CDC SA&A SOP*, if applicable. Also see the sections of this contract concerning "Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA)" and "Requirements for Procurements Involving Privacy Act Records."

  NOTE: If social security numbers (SSN) are expected to be handled by the system, the program and Contractor must include a *SSN Elimination or Usage Approval Request* along with the PTA/PIA. That request will be processed in accordance with the *OCISO Standard for Limiting the Use of Social Security Numbers in CDC Information Systems*.

- **System Security Plan (SSP) –** The SSP must be provided in a digital format supporting copy or export of all content into the HHS/CDC automated SA&A tool. 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 and CDC policies and other guidance. The SSP shall be consistent with and detail the approach to IT security contained in the Contractor's bid or proposal that resulted in the award of this contract. The SSP shall provide an overview of the system environment (including an inventory of all devices and software contained within the system boundary) and security requirements to protect 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.
- **Risk Assessment Report (RAR)** The initial security assessment shall be conducted by the Contractor in conjunction with the program's Information System Security Officer, consistent with NIST SP 800-53A, NIST SP 800-30, and HHS and CDC policies. The assessor will document and submit the assessment results in the RAR, in accordance with the process and formats described in the *CDC SA&A SOP*. 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) for CDC OCISO approval in accordance with the *CDC SA&A SOP*. Thereafter, the Contractor, in coordination with *CDC* shall conduct an assessment of the security controls and update the RAR within 365 days.

POA&M –The POA&M shall be documented consistent with the HHS Standard for Plan of Action and Milestones and CDC policies. 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 Security Assessment Report (SAR), shall be documented and tracked by the Contractor for mitigation in the POA&M document. Depending on the severity of the risks, CDC 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 and CDC 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 Assessment** – 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; NIST SP 800-63, *Digital Identity Guidelines;* the *OCISO Standard for Electronic Authentication (E-Authentication); and* the *CDC SA&A SOP*.

  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 by specified due date.
- **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 annually. 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 annually. The contractor shall maintain a capability to provide security configuration compliance information for 100% of its IT assets using SCAP-compliant automated tools.
- **Vulnerability Management -** 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 annually.
- **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 timeline per OCISO Vulnerability Remediation Framework Standard.
- **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).

1) **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.

2) **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*.
3) **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 information categorized as moderate or high impact as required by OMB Memorandum A-130, *Managing Information as Strategic Resource*, in accordance with the HHS *Standard for Encryption of Computing Devices and Information* and FIPS 140-2.
   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) **Change Management.** Once a system is authorized, all changes must be approved by CDC in

accordance with NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations;* the *HHS IS2P;* and the timeline, process and formats proscribed in the CDC *OCISO Change Management Standard Operating Procedure*.

5) **Retirement / Decommissioning.** When the CDC program and Contractor determine the system is no longer required, it must be decommissioned in accordance NIST SP 800-88, *Guidelines for Media Sanitization*; the *HHS IS2P;* and the timeline, process and formats proscribed in the CDC *OCISO System Retirement Standard Operating Procedure*.

Standard-4: Contracts Involving Cloud Services

A. HHS FedRAMP Privacy and Security Requirements

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

1) **FedRAMP Compliant ATO**. Comply with FedRAMP Security Assessment and Authorization (SA&A) requirements and ensure the information system/service under this contract has a valid FedRAMP compliant (approved) authority to operate (ATO) in accordance with Federal Information Processing Standard (FIPS) Publication 199 defined security categorization. If a FedRAMP compliant ATO has not been granted, the Contractor shall submit a plan to obtain a FedRAMP compliant ATO.
   a. Implement applicable FedRAMP baseline controls commensurate with the agency-defined security categorization and the applicable FedRAMP security control baseline (www.FedRAMP.gov). The *HHS Information Security and Privacy Policy (IS2P)* and *HHS Cloud Computing and Federal Risk and Authorization Management Program (FedRAMP) Guidance* further define the baseline policies as well as roles and responsibilities. The Contractor shall also implement a set of additional controls identified by the agency when applicable.
   b. A security control assessment must be conducted by a FedRAMP third-party assessment organization (3PAO) for the initial ATO and annually thereafter or whenever there is a significant change to the system's security posture in accordance with the FedRAMP Continuous Monitoring Plan.
2) **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.
3) **Service Level Agreements.** *Add when applicable* The Contractor shall understand the terms of the service agreements that define the legal relationships between cloud customers and cloud providers and work with CDC to develop and maintain an SLA.
4) **Interconnection Agreements/Memorandum of Agreements.** *Add when applicable* The Contractor shall establish and maintain Interconnection Agreements and or Memorandum of Agreements/Understanding in accordance with HHS/CDC policies.

B. 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 protect it to the same extent they would the proprietary data and/or company trade secrets and in accordance with HHS/CDC 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 FedRAMP requirements and HHS 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/CDC. 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 contract language herein related to "Requirements for Procurements Involving Privacy Act Records".

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

1) The Contractor (and/or any subcontractor) shall comply with HHS and FedRAMP 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/CDC security policies and in accordance with the contract language herein related to "Procurements Involving Government Information Processed on GOCO or COCO Systems".
   a. In addition to the FedRAMP compliant ATO, the contractor shall complete and maintain an agency SA&A package to obtain agency ATO prior to system deployment/service implementation in accordance with the contract language herein related to "Procurements Involving Government Information Processed on GOCO or COCO Systems". The agency ATO must be approved by the CDC Authorizing Official (AO) prior to implementation of system and/or service being acquired.
   b. CSP systems must leverage a FedRAMP accredited third-party assessment organization (3PAO).
   c. For all acquired cloud services, the SA&A package must contain documentation in accordance with the contract language herein related to "Procurements Involving Government Information Processed on GOCO or COCO Systems". Following the initial ATO, the Contractor must review and maintain the ATO in accordance with HHS/CDC policies.
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 FedRAMP 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 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 For all system-level weaknesses, the following are specified mitigation timelines from weakness creation date in the POA&M:
    a. **30 days** for critical weaknesses;
    b. **60 days** for high weaknesses;
    c. **180 days** for medium weaknesses; and
    d. **365 days** for low weakness.
    e. HHS will determine the risk rating of vulnerabilities using FedRAMP baselines.
5) **Revocation of a Cloud Service**. HHS/[CDC/OCIO] have 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 and FedRAMP security and privacy requirements and/or there is an incident involving sensitive information, HHS and/or *[CDC]* 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.

C. Reporting and Continuous Monitoring

1) Following the initial ATOs, the Contractor (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 Contractor must provide the following artifacts/deliverables on a ***monthly*** basis:
    a. Vendor/Contractor that owns infrastructure where the system resides:
        i. Perform periodic Authenticated Vulnerability Scans and Application Scans (if applicable) according to OCISO ISCM guidance
        ii. Perform weekly scans (at a minimum) and provide results to C/I/O/ISSO and OCISO ISCM for systems with a FIPS 199 impact level of High, HVA, or if the system contains PII, and ensure scan results are submitted in either CSV or PDF format
        iii. Remediate vulnerabilities in accordance with OCISO Vulnerability Remediation Framework Policy
        iv. Advise the C/I/O/ISSO for any instance when critical/high vulnerabilities cannot be remediated as in accordance with the OCISO Vulnerability Framework Standard
        v. Submit monthly Authenticated Vulnerability scans and Application scans (if applicable) to CDC (business owner) and C/I/O/ISSO
    b. Business Stewards (such as System Owner):
        i. Confirm Vendor/Contractor is performing Authenticated Vulnerability Scans and Application Scans (if applicable) according to OCISO ISCM guidance
        ii. Review monthly Authenticated Vulnerability Scans and Application Scans (if applicable); Develop POA&Ms as needed
        iii. Submit monthly Authenticated Vulnerability Scans and Application Scans (if applicable) to OCISO ISCM

iv. Submit written waiver requests to the CISO when systems cannot comply with the provisions of this standard
v. Track remediation/mitigation of security gaps to closure

c. Operating system, database, Web application, and network vulnerability scan results;
d. Updated POA&Ms;
e. Any updated authorization package documentation as required by the annual attestation/assessment/review or as requested by the System Owner or AO; and
f. Any configuration changes to the system and/or system components or CSP's cloud environment, that may impact HHS/CDC'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.

D. Configuration Baseline

1) The contractor 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/CDC configuration baseline.
2) The 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.

E. Incident Reporting

Include Incident Response language from Section 2

1) The Contractor (and/or any subcontractor) shall provide an Incident and Breach Response Plan (IRP) in accordance with HHS CDC, OMB, and US-CERT requirements and obtain approval from the CDC. In addition, the Contractor must follow the incident response and US-CERT reporting guidance contained in the FedRAMP Incident Communications.
2) 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/CDC personnel, or agents acting on behalf of HHS/CDC, 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 Protoeol (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.

F. 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 protect the confidentiality, integrity, and availability of all government information transported outside of controlled facilities.

G. 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.

52.217-9 Option to Extend the Term of the Contract.

As prescribed in 17.208(g), insert a clause substantially the same as the following:

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 10 days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 10 days before the contract expires. The preliminary notice does not commit the Government to an extension.

(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 24 months.

(End of clause)

SECTION C – PERFORMANCE WORK STATEMENT

Media Monitoring - NCIPC

I. Background and Need:

For more than 20 years, CDC's National Center for Injury Prevention and Control (the Injury Center) has helped protect Americans from injuries and violence. We are the nation's leading authority on injury and violence. We study violence and injuries and research the best ways to prevent them, applying science and creating real-world solutions to keep people safe, healthy, and productive. In the United States, injury is the leading cause of death for children and adults between the ages of 1 and 45. Injuries and violence affect everyone—regardless of age, race, or economic status. More than 3 million people are hospitalized, 27 million people are treated in emergency departments and released, and over 192,000 die as a result of violence and unintentional injuries each year.

- Adverse Childhood Experiences (ACEs) are potentially traumatic events that occur in childhood. ACEs can include violence, abuse, and growing up in a family with mental health or substance use problems. Toxic stress from ACEs can change brain development and affect how the body responds to stress. ACEs are linked to chronic health problems, mental illness, and substance misuse in adulthood. Preventing ACEs could reduce a large number of health conditions, including depression, heart disease and overweight/obesity.

- Suicide is a serious public health problem that can have lasting harmful effects on individuals, families, and communities. Suicide is more than a mental health concern. Suicide is a public health problem because of its far-reaching effects. Suicide is the 10th leading cause of death in the United States.

- Drug overdose deaths continue to impact communities in the United States. From 1999 to 2019, nearly 841,000 people have died from a drug overdose. In 2019, more than 70,000 people died from drug overdoses, making it a leading cause of injury-related death in the United States. Opioids were involved in 49,860 overdose deaths in 2019 (70.6% of all drug overdose deaths). 136 Americans die every day from an opioid overdose.

II. Project Objective:

Media monitoring provides data to drive decisions crucial for achieving the mission of the Injury Center. The Office of Communication (OC) within Injury Center provides communication leadership and support in order to prevent violence and unintentional injury and to reduce their consequences.

- Leads planning efforts for communication projects across the Center;
- Develops a variety of communication products;
- Oversees the Center's branding efforts;
- Conducts audience analysis;
- Develops and tests appropriate messages:
- Conducts media planning and evaluation; and
- Develops digital communication and marketing strategies.

With limited resources, it is critical that the Injury Center target digital media communications, partnership, and outreach efforts where they will be most effective. The purpose of this task order is to obtain media monitoring services to track the growing number of priority topic mentions across all media; to track the reach of articles and data releases; have an archive of media mentions; and, to provide a newsletter and archive of all media mentions. CDC's Injury Center receives approximately 1200 media requests per year and that number has been significantly increasing every year since 2014. Monitoring is needed on a variety of topics including child abuse, domestic violence, sexual assault, youth violence, school violence, firearm violence, drug overdose, motor vehicle crashes, suicide, poisoning, traumatic brain injury, falls, fires, marijuana, and may more.

III. Description of Work - Media Monitoring

News Exposure is a subscription news monitoring system. It provides 12 months of the following:

MONITORING DASHBOARD – Up to 5 unique user profiles.

BROADCAST MONITORING – Monitoring of all 210 local U.S. DMA. Broadcast monitoring includes local market newscasts, nationally televised, syndicated content and cable news and cable programming. Monitoring includes top 350+ terrestrial radio stations.

INTERNET NEWS MONITORING - Monitoring of 50,000+ news websites including the online editions of newspapers, magazines, trade publications, journals as well as television and radio station websites. Monitoring includes millions of U.S. blogs.

EXPRESS PRINT MONITORING - Monitoring of 10,000+ print sources including top U.S. daily newspapers, magazines and trade publications.

UNLIMITED WEB-RESOLUTION NEWS CLIPS - Self-edit and download unlimited web resolution news clips. Set video start and stop points and create downloadable files.

MEDIA COVERAGE – All monitoring results are filtered for accuracy via custom Boolean searches. Video & audio previews for TV/Radio are available for a minimum of 90 days from the airdate. Links to websites are available until content is removed by site webmaster. Ability to export coverage and share results.

MEDIA ARCHIVE - All purchased or self-edited news clips will be stored in the cloud. View, share or download your clips any time. For the duration of this agreement, your archive videos remain on our server.

MEDIA POWERSEARCH - Unlimited searching via the News Exposure broadcast and internet news search engine. Access closed caption summaries of entire broadcasts, view internet news articles, save coverage results or export search results into custom reports. Ability to back-search broadcast coverage to 2002 and approximately one calendar year for internet news coverage.

DAILY NEWS ALERTS - Receive daily email alerts detailing air date, time, station, newscast text summaries, preview video & audio, Nielsen audience numbers and publicity values for broadcast content. Internet news summaries include date, time of publication, publication name, link to web article and internet metrics.

UNLIMITED KEYWORDS - Includes set up of ongoing searches, keywords can be modified any time to meet National Center for Injury Prevention and Control's needs

DEDICATED SUPPORT– News Exposure provides a dedicated senior account executive to support and maintain the well-being of the National Center for Injury Prevention and Control's account.

CUSTOM NEWSLETTER - News Exposure's analysts will filter coverage results and compose a bi-weekly newsletter comprised of key media hits sorted according to National Center for Injury Prevention and Control's topic profiles. Reports delivered by 2pm ET on report due dates. 104 Newsletters

Information Security and Privacy Requirements

Baseline Security Requirements

a. **Applicability**. The requirements herein apply whether the entire contract or order (hereafter "contract), or portion thereof, includes either or both of the following:

1) 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.

2) Operate a Federal System Containing Information: A Contractor (and/or 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 design to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources.

b. **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:

1) Protect 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.

2) 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.

3) 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 (IS2), by contacting the CO/COR or emailing fisma@hhs.gov.

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

c. **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:	[X] Low [] Moderate [] High
Integrity:	[] Low [X] Moderate [] High
Availability:	[X] Low [] 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 [X] Low [] Moderate [] High

d. **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 "handling" 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. 633123. All sensitive information that has been identified as CUI by a regulation or statute, handled by this solicitation/contract, shall be:

1) marked appropriately;

2) disclosed to authorized personnel on a Need-To-Know basis;

3) 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

4) 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.*

e. **Protection of Sensitive Information**. For security purposes, information is *or* may be sensitive because it requires security to protect its confidentiality, integrity, and/or availability. The Contractor (and/or any subcontractor) shall protect 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.

f. **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 and *[CDC]* policies. Unauthorized disclosure of information will be subject to the HHS/*[CDC]* 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).

g. **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).*

h. **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 protect against attacks that attempt to downgrade connections to plain HTTP. For internal-facing websites, the HTTPS is not required, but it is highly recommended.

i. **Contract Documentation**. The Contractor shall use provided templates, policies, forms and other agency documents to comply with contract deliverables as appropriate.

j. **Standard for Encryption Language.** The Contractor (and/or any subcontractor) shall:

1) Comply with the *HHS Standard for Encryption of Computing Devices and Information* to prevent unauthorized access to government information.

2) 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.

3) Secure all devices (i.e.: desktops, laptops, mobile devices, etc.) that store and process government information and ensure devices meet HHS and CDC-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).

4) 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.

5) 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 CDC Office of Chief Information Security Officer (OCISO).

k. **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 CDC 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.

l. **Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA)** – The Contractor shall assist the CDC Senior Official for Privacy (SOP) or designee with conducting a PTA for the information system and/or information handled under this contract in accordance with HHS policy and OMB M-03-22, Guidance for Implementing the Privacy Provisions of the E- Government Act of 2002.

1) If the results of the PTA show that a full PIA is needed, the Contractor shall assist the CDC SOP or designee with completing a PIA for the system or information within 30 days 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*.

2) The Contractor shall assist the CDC 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 CDC SOP that a review is required based on a major change to the system (e.g., new uses of information collected, changes to the way information is shared or disclosed and for what purpose, or when new types of PII are collected that could introduce new or increased privacy risks), whichever comes first.

m. 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/CDC 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 *CDC Security Awareness Training (SAT), 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 (RBT) ***within 60 days*** of assuming their new responsibilities. Thereafter, they shall complete RBT at least ***annually*** in accordance with HHS policy and the *HHS Role-Based Training (RBT) of Personnel with Significant Security Responsibilities Memorandum*.
All HHS employees and contractors with SSR who ***have not*** completed the required training within the mandated timeframes shall have their user accounts disabled until they have met their RBT requirement.

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.

n. 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 *CDC 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.

o. 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)/CDC CSIRT 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.

OMB Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information" (03 January 2017) further adds:

A breach is not limited to an occurrence where a person other than an authorized user potentially accesses PII by means of a network intrusion, a targeted attack that exploits website vulnerabilities, or an attack executed through an email message or attachment. A breach may also include the loss or theft of physical documents that include PII and portable electronic storage media that store PII, the inadvertent disclosure of PII on a public website, or an oral disclosure of PII to a person who is not authorized to receive that information. It may also include an authorized user accessing PII for another 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".

Contracts with entities that collect, maintain, use, or operate Federal information or information systems on behalf of CDC shall include the following requirements:

1) The contractor shall cooperate with and exchange information with CDC officials, as deemed necessary by the CDC Breach Response Team, to report and manage a suspected or confirmed breach.

2) All contractors and subcontractors shall properly encrypt PII in accordance with OMB Circular A-130 and other applicable policies, including CDC-specific policies, and comply with HHS-specific policies for protecting PII. To this end, all contractors and subcontractors shall protect all sensitive information, including any PII created, stored, or transmitted in the performance of this contract to avoid a secondary sensitive information incident with FIPS 140-2 validated encryption.

3) All contractors and subcontractors shall participate in regular training on how to identify and report a breach.

4) All contractors and subcontractors shall report a suspected or confirmed breach in any medium as soon as possible and no later than 1 hour of discovery, consistent with applicable CDC IT acquisitions guidance, HHS/CDC and incident management policy, and United States Computer Emergency Readiness Team (US-CERT) notification guidelines. To this end, the Contractor (and/or any subcontractor) shall respond to all alerts/Indicators of Compromise (IOCs) provided by HHS Computer Security Incident Response Center (CSIRC) or CDC Computer Incident Response Team (CSIRT) within 24 hours via email or telephone at whether the response is positive or negative.

5) All contractors and subcontractors shall be able to determine what Federal information was or could have been accessed and by whom, construct a timeline of user activity, determine methods and techniques used to access Federal information, and identify the initial attack vector.

6) All contractors and subcontractors shall allow for an inspection, investigation, forensic analysis, and any other action necessary to ensure compliance with HHS/CDC Policy and the HHS/CDC Breach Response Plan and to assist with responding to a breach.

7) Cloud service providers shall use guidance provided in the FedRAMP Incident Communications Procedures when deciding when to report directly to US-CERT first or notify CDC first.

8) Identify roles and responsibilities, in accordance with HHS/CDC Breach Response Policy and the HHS/CDC Breach Response Plan. To this end, the Contractor shall NOT notify affected individuals unless and until so instructed by the Contracting Officer or designated representative. If so, instructed by the Contracting Officer or representative, all notifications must be pre- approved by the appropriate CDC officials, consistent with HHS/CDC Breach Response Plan, and the Contractor shall then send CDC- approved notifications to affected individuals; and,

9) Acknowledge that CDC will not interpret report of a breach, by itself, as conclusive evidence that the contractor or its subcontractor failed to provide adequate safeguards for PII.

p. 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).

q. 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.*

For additional information, see HSPD-12 policy at: https://www.dhs.gov/homeland-security-presidential- directive-12

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 by the effective date of this contract. Any revisions to the roster as a result of staffing changes shall be submitted immediately upon 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.

r. Contract Initiation and Expiration

1) **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: https://www.hhs.gov/ocio/ea/documents/proplans.html
CDC EPC Requirements: https://www2a.CDC.gov/CDCup/library/other/eplc.htm

2) **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.

3) **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*.

4) **Notification.** The Contractor (and/or any subcontractor) shall notify the CO and/or COR and system ISSO before an employee stops working under this contract.

5) **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 *CDC* policies.

6) The Contractor (and/or any subcontractor) shall perform and document the actions identified in the CDC Out-Processing Checklist (http://intranet.cdc.gov/od/hcrmo/pdfs/hr/Out_Processing_Checklist.pdf) when an employee terminates work under this contract. All documentation shall be made available to the CO and/or COR upon request.

s. Records Management and Retention

The Contractor (and/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/CDC policies and shall not dispose of any records unless authorized by HHS/CDC.

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/CDC policies.

Performance Work Statement
COVID-19 Social Media Ad Support

I. Background and Need:

CDC's COVID-19 response activity works to ensure that all CDC audiences are provided with credible, timely and accurate information in order to prevent further spread of COVID-19. OADC is providing support for the Joint Information Center (JIC) Social Media team as well as the primary CDC social media channels. Expanding CDC's reach to its social media audiences is a key communication strategy.

II. Project Objective:

The objective of this task order is to secure social media services for managing and implementing COVID-19 social media buying strategies. The focus of this work is to expand the reach of CDC's existing social media assets.

This work will ensure that expanded audiences will receive social media information tailored for those channels through effective social media ads.

III. Description of Work

The contractor shall support developing a social media ad buy strategy, procurement of the ads, implementation of the ads, and evaluation. Ads must be supported for all social media channels including Twitter, Instagram, YouTube, Snap Chat, LinkedIn or other proposed platforms. CDC currently has an in-kind gift on its Facebook platform.

Task 1. Project Management

a. Kickoff Meeting - A kickoff meeting shall be held no later than 10 work days after the initial award is made to discuss plans and timelines as well as clarify roles and responsibilities, to be held via phone.
b. Work Plan - Following the kickoff meeting, the contractor shall develop a short-written work plan, including all essential interim and final deliverables, key staff responsible for tasks (including contractor, CDC or other partners), and schedule of key deadlines (including review cycles and absolute No Later Than (NLT) dates for key activities and deliverables) for COR review and correction before acceptance. The work plan must contain:

a. A list confirming the reports and activities proposed by the contractor
b. contractor plan for employee management including how the contractor must avoid any appearances of personal services by the CDC, and
c. schedule for Estimate at Complete (EACs)
d. plan to ensure accuracy of all ads posted and assurance all content has been cleared and approved.

The work plan is due no later than 10 work days following the kickoff meeting. The work plan (and any schedule of interim deliverables) may be revised according to CDC acceptance of the updated work plan by the COR during the project with the restriction that these changes must not impact the overall period of performance, scope, or specifications of the award, or otherwise impinge on the authority of the contracting officer. It is the responsibility of the contractor to fully understand what changes require contracting officer approval.

c. Quarterly Conference Call – A quarterly conference call with CDC COR, must be held. The meeting shall be initiated and led by the contractor. The purpose of this call is ongoing review of task performance. The discussion from the conference call must be documented via e-mail after the meeting. Any required performance improvements must be documented/reported via e-mail to the COR after the meeting.

Task 2. Develop a social media ad buy plan for COVID-19

The Contractor shall develop and submit for Task Order COR approval, a plan setting forth a suggested social media ad strategy to include platforms and target audiences. The plan must be developed in consultation with appropriate CDC offices and/or other contractors. The plan shall provide for the cost-effective, paid placements of materials on social media platforms. The plan must specify for a given level of total advertising expenditure, the recommended media mix to achieve maximum communication impact with CDC's target audience. The plan shall focus on extending the reach of existing CDC social media. The plan must be adjusted as priorities change and in consultation with the COR. A draft plan is due 20 days after award. The plan shall be reviewed bi-monthly and revised based on CDC's communication priorities.

Task 3. Implement and manage social media ad buys for COVID-19

The contractor shall manage all ad buys within CDC's social media profile's ad management systems (such as Twitter's ad manager). This contractor shall procure an average of $65,000 of ad buys per month. CDC and the vendor may vary this monthly spend depending on volume needs but the total ads per year must remain the same.

Support activities for this task shall include:

1. Selecting ad content from existing CDC's organic social media content, CDC/HHS or other federal COVID campaigns (such as the Ad Council content)
2. Identifying needs for new content if organic content is unavailable to meet the ad strategy objectives.
3. Ensuring that ads are optimized for the social platform where the ads are running.
4. Drafting and clearing the content through CDC's Joint Information Center (JIC) if new or edited content or visual design is required.
5. Working with CDC's in-house graphic design team on any needed visual designs, if needed
6. Ensuring ads are approved by the platform ad management system.
7. Monitoring ad activity closely and monitor all Ad comments. If comment responses are needed, secure answers through the JIC Social media team.
8. Support for both English and Spanish ad management.

The vendor shall provide the COR and JIC Social media leads a weekly schedule of all ad content for approval along with proposed ad expenditures. This schedule shall be provided 1 week in advance of any proposed activity.

Task 4. Evaluate, Consult and Report on Ad performance

The contractor must support CDC in effective ad performance. The contractor shall:

1. Evaluate how well ads are performing and make recommendations, as needed, to adjust the strategy.
2. The contractor shall provide weekly metrics reports on ads performance to include key

metrics such as reach, cost per result, amount spent, engagement, and shares. Reports shall include metrics on funding still available for ads through this contract as well as other social media ad buys. The COR and JIC Social Media lead must approve format of the first report.

3. Participate in JIC Social Media team meetings via phone one time per week to discuss ad strategies and CDC social media priorities to inform the ad strategy.

IV. Deliverables:

All task order deliverables intended for communication to the public must comply with Public Law 111–274, the Plain Writing Act of 2010. For Plain Language information and the Federal Plain Language Guidelines see www.plainlanguage.gov.

Task No.	Deliverable	Quantity	Delivery Method	Deliver To	Due Date
1	Kickoff Meeting	1 (per year)	Electronically via E-mail	COR and JIC Social Media Leads	10 working days following award
1	Work Plan	1 (per year)	Electronically via E-mail	COR and JIC Social Media Leads	10 working days following kickoff meeting
1	Quarterly Conference Call	4 (per year)	Electronically via E-mail	JIC Social Media Leads	Within the last 4 weeks of the end of each quarter
2	Ad buy strategy	12 (one per month)	Electronically via E-mail	JIC Social Media Leads	First draft due 20 days after award. Revised monthly based on CDC communication priorities.
3	Ad published	Average of $65,000 in ads (Per month)	Social media ad manger platforms	JIC Social Media leads	Daily management on business days
4	Ad monitoring reports	Daily (5 per week, business days only)	n/a	JIC Social Media leads	Daily management on business days
3	Weekly ad schedule report	1 (per week)	Electronically via E-mail	JIC Social Media Leads	1 week in advance of when ads start to run.
4	Weekly metrics report	1 (per week)	Electronically via E-mail	JIC Social Media Leads with copy to COR	1 week after ads have run

All materials must be submitted electronically in MS compatible format that meets CDC standards and is readily available at CDC (e.g. MS Office (Word, Excel, PowerPoint) or Adobe Acrobat. All reporting requirements and written deliverables as part of this contract will be supplied to the project Contracting Officer Representative (COR). Acceptance of any written deliverables is pending CDC COR review and correction to any resulting comments, to be confirmed in writing and documented via e-mail to the COR. Any schedule of interim deliverables may be revised according to CDC acceptance of an updated written work plan by the COR during the project with the restriction that these changes must not impact the overall period of performance, scope, or specifications of the award, or otherwise impinge on the

authority of the contracting officer. It is the responsibility of the contractor to fully understand what changes require contracting officer approval.

V. Performance Matrix:

Work Requirement	Acceptable Quality Level (AQL)	Monitoring Method	Incentives/ Disincentives
Task 1 Kick off meeting (base year and repeated annually)	• Occurs at regularly scheduled times • Contractor is prepared to discuss relevant project issues, is responsive to project planning issues/project improvments, and documents meetings as described in PWS (may be corrected to COR comments)	• 100% review of event (by the COR) • Unacceptable meetings will be documented as customer complaints, contractor may be allowed to correct any insufficiences to CDC satisfaction	• Contractor's performance is documented as past performance using CPARS which is considered for future awards. • Performance is considered in determining whether to exercise the option periods • Repeated complaints on different events/tasks but the same issue will be elevated for higher level resolution (senior management and/or OAS)
Task 1 Work Plan	• Appropriate content is included as outlined in the PWS • Appropriate content is included as outlined in the PWS (may be corrected to COR comments)	• 100% review of delivered reports (by the COR) • Unacceptable quarterly conference meetings will be documented as customer complaints, contractor may be allowed to correct any insufficiences to CDC satisfaction	

Work Requirement	Acceptable Quality Level (AQL)	Monitoring Method	Incentives/ Disincentives
Task 1 Quarterly Conference Calls	• Occurs at regularly scheduled times (100% within schedule) • Contractor is prepared to discuss relevant work performance, is responsive to performance issues, and documents quarterly meetings as described in PWS	• 100% review of events (by the COR) • Unacceptable quarterly conference meetings will be documented as customer complaints, contractor may be allowed to correct any insufficiences to CDC satisfaction	
Task 2: Ad buy strategy	• Appropriate content is proposed as outlined in the PWS • Appropriate content is based on best practies in social media ad and based on CDC's communication goals	• 100% review of strategy (by the COR) • Unacceptable ad buy strategy will be documented as customer complaints, contractor may be allowed to correct any insufficiences to CDC satisfaction	
Task 3: Manage ad buys	• Ads Only CDC cleared content is posted as ads (100% within compliance). • Ads are error free (100% within complaince) • Ads meet goals determined in CDC's ad strategy • Ads run as scheduled • Proposed weekly	• 100% review of weekly schedule (by the JIC Social Media leads) • Posted uncleared content or content with errors will be document as a major customer complaint. • Repated unacceptable weekly schedules will be documented as customer complaints, contractor may be	

Work Requirement	Acceptable Quality Level (AQL)	Monitoring Method	Incentives/ Disincentives
	schedules require minor edits (85% within complaince)	allowed to correct any insufficiences to CDC satisfaction	
Task 4: Ad metrics reports	• Appropriate metrics are included as jointly determined at the start of the contract • Metrics are accurate	• 80% review of metrics reports (by the JIC Social Media leads) • Unacceptable reports will be documented as customer complaints, contractor may be allowed to correct any insufficiences to CDC satisfaction	

VI. Period of Performance:

The period of performance is:

Year 1 (Basic Period): 04/01/2022-3/31/2023

VII. Place of Performance:

Work shall be performed at the contractor's facilities. Work can be remote.

VIII. Government Furnished Materials, Facilities and Property

CDC will provide network access and equipment for contract staff administering ads.

IX. Information Security and Privacy 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) employee 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. Protect 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:	[X] Low [ ] 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:

[ ] No PII [X] Yes PII

4) **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

5) **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*.

6) **Protection of Sensitive Information**. For security purposes, information is *or* may be sensitive because it requires security to protect its confidentiality, integrity, and/or availability. The Contractor (and/or any subcontractor) shall protect 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.

7) **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 and CDC policies. Unauthorized disclosure of information will be subject to the HHS/CDC 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).

8) **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)*. .

9) **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 protect against attacks that attempt to downgrade connections to plain HTTP. For internal-facing websites, the HTTPS is not required, but it is highly recommended.

10) **Contract Documentation**. The Contractor shall use provided templates, policies, forms and other agency documents to comply with contract deliverables as appropriate.

11) **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, pris, 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 and CDC-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 bave 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 *[CDC-provided delivery date]*.

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 CDC Office of Chief Information Security Officer (OCISO).

12) **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 CDC 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.

13) **Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA)** – The Contractor shall assist the CDC Senior Official for Privacy (SOP) or designee with conducting a PTA for the information system and/or information handled under this contract in accordance with HHS policy and OMB M-03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.

a. The Contractor shall assist the CDC 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 CDC SOP that a review is required based on a major change to the system (e.g., new uses of information collected, changes to the way information is shared or disclosed and for what purpose, or when new types of PII are collected that could introduce new or increased privacy risks), whichever comes first.

B. 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/CDC 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 *CDC Security Awareness Training (SAT)* 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 (RBT) ***within 60 days*** of assuming their new responsibilities. Thereafter, they shall complete RBT at least ***annually*** in accordance with HHS policy and the *HHS Role-Based Training (RBT) of Personnel with Significant Security Responsibilities Memorandum*.

All HHS employees and contractors with SSR who ***have not*** completed the required training within the mandated timeframes shall have their user accounts disabled until they have met their RBT requirement.

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.

C. 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 *CDC 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.

D. Incident Response

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.
OMB Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information" (03 January 2017) states:

Definition of an Incident:
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.
Definition of a **Breach:**
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.
It further adds:

A breach is not limited to an occurrence where a person other than an authorized user potentially accesses PU by means of a network intrusion, a targeted attack that exploits website vulnerabilities, or an attack executed through an email message or attachment. A breach may also include the loss or theft of physical documents that include PU and portable electronic storage media that store PU, the inadvertent disclosure of PU on a public website, or an oral disclosure of PII to a person who is not authorized to receive that information. It may also include an authorized user accessing PU 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".

Contracts with entities that collect, maintain, use, or operate Federal information or information systems on behalf of CDC shall include the following requirements:

1) The contractor shall cooperate with and exchange information with CDC officials, as deemed necessary by the CDC Breach Response Team, to report and manage a suspected or confirmed breach.

2) All contractors and subcontractors shall properly encrypt PII in accordance with OMB Circular A-130 and other applicable policies, including CDC-specific policies, and comply with HHS-specific policies for protecting PII. To this end, all contractors and subcontractors shall protect 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.

3) All contractors and subcontractors shall participate in regular training on how to identify and report a breach.

4) All contractors and subcontractors shall report a suspected or confirmed breach in any medium as soon as possible and without unreasonable delay, consistent with applicable CDC IT acquisitions guidance, HHS/CDC and incident management policy, and United States Computer Emergency Readiness Team (US-CERT) notification guidelines. To this end, the Contractor (and/or any subcontractor) shall respond to all alerts/Indicators of Compromise (IOCs) provided by HHS Computer Security Incident Response Center (CSIRC) or CDC Computer Incident Response Team (CSIRT) within 24 hours via email at cdc@csirt.gov or telephone at 866-655-2245, whether the response is positive or negative.

5) All contractors and subcontractors shall be able to determine what Federal information was or could have been accessed and by whom, construct a timeline of user activity, determine methods and techniques used to access Federal information, and identify the initial attack vector.

6) All contractors and subcontractors shall allow for an inspection, investigation, forensic analysis, and any other action necessary to ensure compliance with HHS/CDC Policy and the HHS/CDC Breach Response Plan and to assist with responding to a breach.

7) Cloud service providers shall use guidance provided in the FedRAMP Incident Communications Procedures when deciding when to report directly to US-CERT first or notify CDC first.

8) Identify roles and responsibilities, in accordance with HHS/CDC Breach Response Policy and the HHS/CDC Breach Response Plan. To this end, the Contractor shall NOT notify affected individuals unless and until so instructed by the Contracting Officer or designated representative. If so instructed by the Contracting Officer or representative, all notifications must be pre-approved by the appropriate CDC officials, consistent with HHS/CDC Breach Response Plan, and the Contractor shall then send CDC- approved notifications to affected individuals; and,

9) Acknowledge that CDC will not interpret report of a breach, by itself, as conclusive evidence that the contractor or its subcontractor failed to provide adequate safeguards for PII.

E. 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).

F. 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 by the effective date of this contract. Any revisions to the roster as a result of staffing changes shall be submitted immediately upon 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.

G. Contract Initiation and Expiration

1) **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).

2) **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.

3) **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*.

4) **Notification.** The Contractor (and/or any subcontractor) shall notify the CO and/or COR and system ISSO before an employee stops working under this contract.

5) **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 *CDC* policies.

6) The Contractor (and/or any subcontractor) shall perform and document the actions identified in the CDC Out-Processing Checklist (http://intranet.cdc.gov/od/hcrmo/pdfs/hr/Out_Processing_Checklist.pdf) when an employee terminates work under this contract. All documentation shall be made available to the CO and/or COR upon request.

H. 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 policies and shall not dispose of any records unless authorized by HHS.
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 policies.

Schedule of Deliverables

Deliverable Title/Description	Due Date
Roster	NLT 5 days after effective date of this contract
Contractor Employee Non-Disclosure Agreement (NDA)	Prior to performing any work on behalf of HHS
Assist in the completion of a PTA/PIA form	In conjunction with contract award
Copy of training records for all mandatory training	In conjunction with contract award and annually thereafter or upon request
Signed ROB for all employees	Initiation of contract and at least annually thereafter
Incident Report (as incidents or breaches occur)	As soon as possible and without reasonable delay and no later than 1 hour of discovery
Incident and Breach Response Plan	Upon request from government
List of Personnel with defined roles and responsibilities	Prior to performing any work on behalf of HHS
Off-boarding documentation, equipment and badge when leaving contract	At contract expiration after the Government's final acceptance of the work under this contract, or in the event of a termination of the contract.
Onboarding documentation when beginning contract.	Prior to performing any work on behalf of HHS
Form or deliverables required by CDC.	At contract expiration.
If the procurement involves a system or cloud service, additional documentation will be required, such as Disposition/Decommission Plan	At contract expiration.

ORDER FOR SUPPLIES OR SERVICES

PAGE 1 OF PAGES 13

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

1. DATE OF ORDER	2. CONTRACT NO. *(If any)*
12/21/2021	75D30122P13070
3. ORDER NO.	**4. REQUISITION/REFERENCE NO.**
	00HCUG15-2022-62289

5. ISSUING OFFICE *(Address correspondence to)*
Centers for Disease Control and Prevention (CDC)
Office of Acquisition Services (OAS)
2900 Woodcock Blvd, MS TCU-4
Atlanta, GA 30341-4004

6. SHIP TO:

a. NAME OF CONSIGNEE
CDC (NCEH)

b. STREET ADDRESS
4770 BUFORD HIGHWAY

c. CITY	d. STATE	e. ZIP CODE
ATLANTA	GA	30341-3717

f. SHIP VIA

7. TO:

a. NAME OF CONTRACTOR
BEASLEY MEDIA GROUP

DUNS NUMBER: 105257600

b. COMPANY NAME

c. STREET ADDRESS
55 WILLIAM T MORRISSEY BLVD

d. CITY	e. STATE	f. ZIP CODE
DORCHESTER	MA	02125-3315

8. TYPE OF ORDER

[X] a. PURCHASE
REFERENCE YOUR:
Please furnish the following on the terms and conditions specified on both sides of this order and on the attached sheet, if any, including delivery as indicated.

[ ] b. DELIVERY
Except for billing instructions on the reverse, this delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above-numbered contract.

9. ACCOUNTING AND APPROPRIATION DATA
93901NM 2512 2022 75-22-0947 5604111101

10. REQUISITIONING OFFICE
HCUG15

11. BUSINESS CLASSIFICATION *(Check appropriate box(es))*
[ ] a. SMALL [X] b. OTHER THAN SMALL [ ] c. DISADVANTAGED [ ] d. WOMEN-OWNED

12. F.O.B. POINT	14. GOVERNMENT B/L NO.	15. DELIVER TO F.O.B. POINT ON OR BEFORE *(Date)*	16. DISCOUNT TERMS
Destination		05/31/2022	Net 30 Days

13. PLACE OF

a. INSPECTION	b. ACCEPTANCE

17. SCHEDULE *(See reverse for Rejections)*

ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	This is a FIRM FIXED PRICE contract. Invoices must be from Contractor in Box 7a, reference contract number in Box 2, and DUNS number from Box 7a. **Send Invoice/Payment to:** Email: cpbapinv@cdc.gov - Fax: (404) 638-5324 Customer Service: (404) 718-8100 **Vendor Contact:** Aaron Cowan Email: (b)(6) **CDC COR:** Lauren Benet, lgd3@cdc.gov (770) 488-0671 **Contracting Officer:** H. Dale Bish, uwo8@cdc.gov , (404) 498-1312 **Contract Spec.:** Samantha J. Bily, qnb7@cdc.gov, (404) 498-2150					

18. SHIPPING POINT	19. GROSS SHIPPING WEIGHT	20. INVOICE NO.	(b)(4)	17(h) TOT. *(Cont. pages)*

21. MAIL INVOICE TO:

SEE BILLING INSTRUCTIONS ON REVERSE

a. NAME
Centers for Disease Control and Prevention (FMO)

b. STREET ADDRESS *(or P.O. Box)*
PO Box 15580 404-718-8100

c. CITY	d. STATE	e. ZIP CODE	(b)(4)	17(i) GRAND TOTAL
Atlanta	GA	303330080		

22. UNITED STATES OF AMERICA *(Signature)* ▶ Howard D. Bish -S
Digitally signed by Howard D. Bish -S
Date: 2021.12.21 14:03:14 -05'00'

23. NAME *(Typed)*
Howard D Bish
TITLE: CONTRACTING/ORDERING OFFICER

SECTION B - SUPPLIES OR SERVICES AND PRICES/COSTS

ITEM	SUPPLIES / SERVICES	QTY/UNIT	UNIT PRICE	EXTENDED PRICE
0001	**CUSTOM PACKAGE: CDC Noise-Induced Hearing Loss PSA** 2022 Monster Jam Tour Event Geo-Fencing, National Targeted Audience Extension, and Video 360 Firm Fixed Price Severable Services Period of Performance: 01/01/2022 – 05/31/2022		(b)(4)	
	Line(s) Of Accounting: 93901NM 2512 2022 75-22-0947 5604111101 (b)(4)			