STATEMENT OF WORK

Title of Project: Clarivate Analytics Software MetaCore/MetaDrug Licenses

C.1 Background and Need –

The Agency for Toxic Substances and Disease Registry (ATSDR) conducts scientific evaluations to assess and predict potential toxicity endpoints and human health risks associated with environmental chemicals. ATSDR has three offices. The Office of Innovation and Analytics (OIA) within ATSDR comprises four offices, including the Simulation Science Section (SSS).

The Office of Innovation & Analytics (OIA) collects, analyzes, and interprets data and disseminates scientific information to enable internal and external partners to make actionable decisions regarding exposure to hazardous substances. OIA provides analytical and modeling expertise, develops new analytical tools, and integrates geospatial science into public health activities.

The Simulation Science Section (SSS) develops and applies computer models to identify the most effective methods for evaluating and mitigating the hazards posed by toxic chemicals. The group's responsibilities include:

- Aiding evaluations of exposures to hazardous chemicals in communities
- Providing estimates of toxicity from exposure to chemicals in the environment, and
- Contributing advice and support to help reduce the impacts of exposure to chemicals

The scientists in the SSS support basic and applied research projects in collaboration with NCEH, government, and academic institutions. Collectively, these projects advance the goal of developing and applying modeled estimates and expertise to reduce the impacts of toxic chemicals on communities.

A current focus is on assessing the toxicity of environmental and emerging chemicals and on developing models that identify genetic changes associated with toxic chemical exposures. SSS staff have initiated several toxicogenomics projects. Toxicogenomics studies how the genome responds to environmental chemicals. The goals of toxicogenomics are 1) to understand the mechanisms behind toxicity and 2) to explain the relationships between environmental or chemical stress and human disease.

MetaCore/MetaDrug is a web-based bioinformatics suite that allows researchers to upload data analysis results from microarray, next-generation sequencing, metabolic,

SAGE, siRNA, microRNA, and screening. It provides functional analysis to identify the most relevant pathways, networks, and cellular processes in the data. Additionally, gene, protein, compound, pathway, and disease maps are available. The MetaCore/MetaDrug license includes easy-to-use, intuitive tools for searching and data visualization, enabling the identification of the most relevant biological pathways, networks, and processes in a "virtual lab."

Clarivate MetaCore/MetaDrug software will assist OIA/SSS and ATSDR program staff with current computational systems biology tools to help accomplish the agency's mission to investigate environmental exposures to hazardous substances in communities. With consistent use, the software license will help model and understand disease pathways and build unrestricted networks of any size and data type to visualize biological relationships and molecular interactions, annotated with mechanisms, directionality, and effects. Also, to identify and validate targets and biomarkers, and to explore biological, chemical, and disease contexts for biological topics of interest using a single comprehensive source of all critical data.

The license will enable ATSDR/OIA/SSS staff to deliver high-quality, context-rich biological systems content, providing essential data and analytics to accelerate scientific research.

C.2 Project Objective –

The objective of this procurement is to obtain the

Clarivate MetaCore/MetaDrug license renewal for use on the SSS. This platform is an instance of SSS. This is used to examine, summarize, and interpret available toxicological and omics studies to determine human exposure levels that may be associated with health effects. Our studies and projects aim to provide sufficient evidence to support a conclusion about a health effect using available data and computational predictions.

C.3 Scope of Work –

The scope of work is to purchase the
Clarivate MetaCore/MetaDrug license for use on the SSS.

The Agency for Toxic Substances and Disease Registry (ATSDR) Simulation Science Section (SSS) presents and publishes its findings in scientific forums and journals on hazardous substances. At SSS, we examine, summarize, and interpret available toxicological and omics studies to determine human exposure levels that may be associated with health effects. Our studies and projects aim to provide sufficient evidence

to support a conclusion about a health effect using available data and computational predictions.

Clarivate provides the best available computational system biology software. Many experts in the field use Clarivate MetaCore/MetaDrug to assemble and analyze human biological networks, a valuable approach for integrating and interpreting high-throughput experimental data. Many other partners and collaborators use this software in research and federal agencies. MetaCore/MetaDrug is unique for its highly configurable platform, enabling customization and optimization. It has been approved and evaluated by our IT personnel. Because MetaCore/MetaDrug is an online platform, it provides easy access and enhances communication around workflows.

C.4 Technical Requirements –

The vendor will provide:

- Clarivate MetaCore/MetaDrug software licenses

C.5 Reporting Schedule –

N/A

C.6 Special Considerations –

Information Security and Privacy Requirements

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

START COPYING LANGUAGE HERE

1. Baseline Security Requirements:
    a. **Applicability.** The requirements herein apply whether the entire contract or modification (hereafter "contract"), or portion thereof, includes either or both of the following:
        i. **Access (Physical or Logical) to Government Information:** A Contractor (and/or any subcontractor) will have or will be given the ability to have, routine physical (entry) or logical (electronic) access to government information.
        ii. **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 CDC 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.

b. **Safeguarding Information and Information Systems.** All government information and information systems must be protected in accordance with HHS/CDC policies and level of risk. At a minimum, the Contractor (and/or any subcontractor) must:
    i. Protect the:
c. **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.
    ii. Categorize all information owned and/or collected/managed on behalf of CDC/*[*CDC Component*]* and information systems that store, process, and/or transmit CDC information 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. Based on information provided by the System Security and Privacy Officer (previously referred to as ISSO), CISO, CDC CPO, or other representative, the impact level for each Security Objective (Confidentiality, Integrity, and Availability) and the Overall Impact Level, which is the highest watermark of the three factors 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 Impact Level:** [x] Low [ ] Moderate [ ] High

iii. Based on the agreed-upon level of impact, implement the necessary safeguards to protect all information systems and information collected and/or managed on behalf of CDC*/[*CDC Component*]* regardless of location or purpose.

iv. Report any discovered or unanticipated threats or hazards by either the agency or contractor, or if existing safeguards have ceased to function immediately after discovery, **within one (1) hour or less**, to the government representative(s).

v. Adopt and implement all applicable policies, procedures, controls, and standards required by the CDC/*[*CDC Component*]* 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 all applicable security and privacy policies by contacting the CO/COR or CDC/*[*CDC Component*]* security and/or privacy officials.

d. **Privacy Act.** Comply with the Privacy Act requirements (when applicable), and tailor FAR and HHSAR clauses as needed.

e. **Privacy Compliance.** Comply with the E-Government Act of 2002, NIST SP 800-53, and applicable CDC Component privacy policies and complete all the requirements below:

i. Per the Office of Management and Budget (OMB) Circular A-130, Personally Identifiable Information (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.

ii. To ensure that the public's personal information is protected in a manner commensurate with the privacy risks, CDC uses a privacy analysis process to assess the risks associated with CDC's collection and maintenance of PII and to ensure information is handled in accordance with applicable legal, regulatory, and policy requirements. PTAs analyze

how information is handled in IT systems and electronic information collections and determines if the IT system or electronic information collection collects, disseminates, maintains, or disposes of PII. PIAs are used to assess the privacy risks of IT systems and electronic information collections that collect, disseminate, maintain, or dispose of PII about members of the public. PIAs also provide transparency into how CDC collects, disseminates, maintains, or disposes of the public's PII.

iii. The Contractor must support the agency with conducting a Privacy Threshold Analysis (PTA) for the information system and/or information handled under this contract to determine whether PII is collected, disseminated, maintained, or disposed as part of the contract. The PTA will determine if a full Privacy Impact Assessment (PIA) needs to be completed.

- If the results of the PTA show that a full PIA is needed, the Contractor must support the agency with completing a PIA for the system or information within *[CDC to insert contract-specific timeline]* after completion of the PTA and in accordance with CDC policy and OMB M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*.
- The Contractor must support the agency 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.

f. **Controlled Unclassified Information (CUI). Executive Order 13556 defines** CUI 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. The requirements below apply only to nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components. All sensitive information that has been identified as CUI by a regulation or statute, handled by this solicitation/contract, must be:

i. Marked appropriately;
ii. Disclosed to authorized personnel on a Need-To-Know basis;
iii. Protected in accordance with NIST SP 800-53, *Security and Privacy Controls for 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,
iv. Returned to HHS/CDC control, destroyed when no longer needed, or held until otherwise directed. Information and/or data must be disposed of in accordance with NIST SP 800-88*, Guidelines for Media Sanitization*.

g. **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) must protect all government information that is or may be sensitive by securing it with a solution that is validated with current FIPS 140 validation certificate from the NIST CMVP.
h. **Confidentiality and Nondisclosure of Information**. Any information provided to the Contractor (and/or any subcontractor) by CDC or collected by the Contractor on behalf of CDC must be used only for the purpose of carrying out the provisions of this contract and must 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 must ensure that all work performed by its employees and subcontractors must be under the supervision of the Contractor. Each Contractor employee or any of its subcontractors to whom any CDC records may be made available or disclosed must 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 must be protected in accordance with HHS/CDC policies. Unauthorized disclosure of information will be subject to the HHS/CDC sanction policies and/or governed by the following laws and regulations:

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

i. **Internet Protocol Version 6 (IPv6).** All procurements using Internet Protocol must comply with OMB Memorandum M-05-22, *Transition Planning for Internet Protocol Version 6 (IPv6)*.
j. **Information and Communications Technology (ICT).** ICT products and services from prohibited entities/sources must not be used/acquired in compliance with Public Law 115- 232, Section 889 Parts A and B, FAR 4.21, FAR 52.204.23, FAR 52.204.24, and FAR 52.204.25. The Contractor (and/or any subcontractor) must notify the government if they identify prohibited ICT products and/or services are used during the contract performance.
k. **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 must enable HTTP Strict Transport Security (HSTS) to instruct compliant browsers to always 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, HTTPS is not required, but it is highly recommended. Consult HHS/CDC Policy for Internet and Email Security for additional information. According to the CDC Web policy, all CDC web content must reside on a CDC.gov domain and must be hosted on CDC or CDC-authorized information systems .
l. **Contract Documentation**. The Contractor must use provided templates, policies, forms, and other agency documents *[*CDC Component*] specify which documents/forms will be provided to contractor]* to comply with contract deliverables as appropriate.
m. **Standard for Encryption.** The Contractor (and/or any subcontractor) must:

i. Comply with the *HHS Standard for*

Encryption of Computing Devices and Information to prevent unauthorized access to government information.

ii. 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 encryption solution that is validated with current FIPS 140 validation certificate from the NIST CMVP.

iii. Secure all devices (i.e.: desktops, laptops, mobile devices, etc.) that store and process government information and ensure devices meet CDC and CDC Component-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).

iv. Verify that the encryption solutions in use have been validated under the Cryptographic Module Validation Program to confirm compliance with current FIPS 140 validation certificate from the NIST CMVP. The Contractor must provide a written copy of the validation documentation to the COR *[*CDC Component- *provided delivery date]*.

v. Use the Key Management system on the CDC 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 http://csrc.nist.gov/publications/. Encryption keys must be provided to CSPO.

n. **Contractor Non-Disclosure Agreement (NDA)**. Each Contractor (and/or any subcontractor) employee having access to non-public government information under this contract must complete the CDC non-disclosure agreement. *[inserted information/link should be cited here]*, as applicable. Contractors (and/or subcontractors) must submit a copy of each signed and witnessed NDA to the Contracting Officer (CO) and/or CO Representative (COR) prior to performing any work under this acquisition.

2. Training Requirements:

a. **Mandatory Training for All Contractor Staff.** All Contractor (and/or any subcontractor) employees assigned to work on

this contract must complete the applicable CDC Contractor Information Security Awareness, Privacy, and Records Management training (provided upon contract award) before performing any work under this contract. Thereafter, the employees must complete *[*CDC Component-*specified]* Information Security Awareness, Privacy, and Records Management training at least ***annually***, during the life of this contract. All provided training must be compliant with CDC training policies.

b. **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/CDC policy and the *CDC Role-Based Training (RBT) of Personnel with Significant Security Responsibilities*.

c. **Training Records.** The Contractor (and/or any subcontractor) must maintain training records for all its employees working under this contract in accordance with CDC policy. A copy of the training records must be provided to the CO and/or COR within ***30 days*** after contract award and ***annually*** thereafter or upon request.

3. Rules of Behavior:
    a. The Contractor (and/or any subcontractor) must ensure that all employees performing on the contract comply with the *CDC Implementation of the HHS Rules of Behavior for Use of HHS Information Technology Resources*, and [*insert any CDC Component-specific rules, as applicable*].
    b. All Contractor employees performing on the contract must read and adhere to the Rules of Behavior before accessing agency 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.
4. Incident Response:
    a. The Contractor (and/or any subcontractor) must respond to all alerts/Indicators of Compromise (IOCs) provided by CDC Computer Security Incident Response Center (CSIRC) IRT teams **within 24 hours,** whether the response is positive or negative. In accordance with FISMA and OMB M-17-12, *Preparing for and Responding to a Breach of Personally*

Identifiable Information (PII)[29], an incident is "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" and a privacy breach is "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." For additional information on the CDC breach response process, please see the *CDC Standard for Responding to Breaches of Personally Identifiable Information (PII)*.[30]"

b. Contracts with entities that collect, maintain, use, or operate Federal information or information systems on behalf of CDC must include in the following requirements:
    i. The Contractor shall cooperate with and exchange information with CDC officials, as deemed necessary by the CDC Breach Response Team, to report and manage of a suspected or confirmed breach.
    ii. 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, with encryption solution that is validated with the current FIPS 140 validation certificate from the NIST CMVP.
    iii. All contractors and subcontractors shall participate in regular training on how to identify and report a breach
    iv. NOT notify affected individuals unless so instructed by the Contracting Officer or designated representative. If instructed by the Contracting Officer or representative, the Contractor must send *[*CDC Component*]* approved notifications to affected individuals [*insert* CDC Component *Specific timeline, process, and format]*.
    v. Report all suspected and confirmed information security and privacy incidents and breaches to the CSPO Incident Response Team (IRT) *[contact*

information should be cited here], COR, CO, CDC CPO (or his or her designee), and other stakeholders, including breaches 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 Component and CDC 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, impact classifications/threat vector, and the type of information compromised. In addition, the Contractor must:

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

vi. Comply with OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information,* and CDC Component and CSPO privacy breach response policies when handling PII breaches.

vii. 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 *[CDC Component insert timeline if required]*.

viii. 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.

ix. 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.

x. 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.

5. Position Sensitivity Designations:
   All Contractor (and/or any subcontractor) employees must obtain a background investigation commensurate with their position sensitivity designation that complies with Parts 1400 and 731 of Title 5, Code of Federal Regulations (CFR). The following position sensitivity designation levels apply to this solicitation/contract.
6. Homeland Security Presidential Directive (HSPD)-12:
   The Contractor (and/or any subcontractor) and its employees must comply with Homeland Security Presidential Directive (HSPD)-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*; OMB M-05-24; OMB M-19-17; FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*; HHS/CDC HSPD-12 policy; and *Executive Order 13467, Part 1 §1.2.*
7. Roster:
   The Contractor (and/or any subcontractor) must 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 must be submitted to the COR and/or CO by *[CDC Component Specific timeline]* of the effective date of this contract. Any revisions to the roster as a result of staffing changes must be submitted immediately upon *[CDC Component Specific timeline]* 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 must provide a position description and the Government will determine the appropriate suitability level.
8. Contract Initiation and Expiration:
   a. **General Security Requirements.** The Contractor (and/or any subcontractor) must comply with information security and privacy requirements, Enterprise Performance Life Cycle (EPLC) processes, CDC 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 must follow the CDC EPLC framework and methodology or *[insert CDC Component-specific requirement]* and in accordance with the CDC Office of Financial Resources (OFR) Contract Closeout Guide and *HHS Closeout Guide: Contracts and Orders.*

b. **System Documentation.** Contractors (and/or any subcontractors) must follow and adhere to CDC System Development Life Cycle requirements, 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.

c. **Sanitization of Government Files and Information.** As part of contract closeout and at expiration of the contract, the Contractor (and/or any subcontractor) must 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*.

d. **Notification.** The Contractor (and/or any subcontractor) must notify the CO and/or COR and System Security and Privacy Officer (previously referred to as ISSO) within *[CDC Component-specific timeline]* before an employee stops working under this contract.

e. **Contractor Responsibilities upon Physical Completion of the Contract**. The Contractor (and/or any subcontractors) must 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 must 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.

f. The Contractor (and/or any subcontractor) must perform and document the actions identified in the *[CDC Component]* Contractor Employee Separation Checklist *[insert links to CDC Component form]* when an employee terminates work under this contract within *[insert CDC Component-specific timeline]* days of the employee's exit from the contract. All documentation must be available to the CO and/or COR upon request.

9. Records Management and Retention:
    a. The Contractor (and/or any subcontractor) must maintain all information in accordance with Executive Order 13556 -- Controlled Unclassified Information, National Archives and Records Administration (NARA) records retention policies and schedules and *CDC Policy for Records Management* and *[CDC Component]* policies and must not dispose of any records unless authorized by CDC/ *[CDC Component]*.
    b. If a Contractor (and/or any subcontractor) accidentally disposes of or destroys a record without proper authorization, he/she must document and report the incident in accordance with CDC/ *[CDC Component]* policies.
10. High Value Asset (HVA):

If a system is identified as HVA, the Contractor must comply with the HHS Policy for the High Value Asset (HVA) Program and the Department of Homeland Security (DHS) HVA Control Overlay in addition to the above requirements.

Section 508 and Accessibility Requirements

Part A – Provision

Reference HHSAR 352.239-73[8] Electronic Information and [Communication] Technology Accessibility Notice.

[(Deviation)]

[(a) Any offeror responding to this solicitation must comply with established HHS Information and Communication Technology (ICT) accessibility standards. Information about Section 508 is available at https://www.hhs.gov/web/section-508/index.html.

(b) The Section 508 accessibility standards applicable to this solicitation are stated in the clause at 352.239-79 Information and Communication Technology Accessibility. In order to facilitate the Government's determination whether proposed ICT supplies, products, platforms, information, and documentation meet applicable Section 508 accessibility standards, offerors must submit an appropriate HHS Section 508 Accessibility Conformance Checklist (see https://www.hhs.gov/web/section-508/accessibility-checklists/index.html) or an Accessibility Conformance Report (ACR) (based on the Voluntary Product Accessibility Template (VPAT) see https://www.itic.org/policy/accessibility/vpat), in accordance with the completion instructions. The purpose of the checklists and conformance reports are to assist HHS acquisition and program officials in determining whether proposed ICT supplies, products, platforms, information, and

documentation conform to applicable Section 508 accessibility standards. Checklists and ACRs evaluate—in detail—whether the ICT conforms to specific Section 508 accessibility standards and identifies remediation efforts needed to address conformance issues.

(c) If an 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, products, platforms, information, documentation, or services support delivered do not conform to the described accessibility standards, remediation of the supplies, products, platforms, information, documentation, or services support to the level of conformance specified in the contract will be the responsibility of the Contractor at its expense.

(d) In order to facilitate the Government's determination whether proposed ICT supplies meet applicable Section 508 accessibility standards, offerors must submit an Accessibility Conformance Report, in accordance with its completion instructions and tailored to the requirements in the solicitation. The purpose of the Report is to assist HHS acquisition and program officials in determining whether proposed ICT supplies conform to applicable Section 508 accessibility standards. The template allows offerors or developers to self-evaluate their supplies and document, in detail, whether they conform to a specific Section 508 accessibility standard, and any underway remediation efforts addressing conformance issues. Instructions for preparing the Template are available at https://www.section508.gov/.

(e) Additionally, offerors must provide enough information to assist the Government in determining that the ICT services conform to Section 508 accessibility standards, including any underway remediation efforts addressing conformance issues.

(f) Respondents to this solicitation must identify any inability to conform to Section 508 requirements. If an 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 described 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.

(g) Items delivered as electronic content must be accessible to HHS acceptance criteria. Checklist for various formats are available at http://508.hhs.gov/. Materials, other than items incidental to contract management, that are final items for delivery should be accompanied by the appropriate checklist, except upon approval of the Contracting Officer or Contracting Officer's Representative.

Part B - Clause

352.239-74[9] Electronic, Information, and Communication Technology Accessibility.

[(Deviation)]

(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 information and communication technology (ICT) supplies, products, platforms, information, documentation, and services, or support developed, acquired, maintained or delivered under this contract or order must comply with the Revised 508 Standards, which are located at 36 C.F.R. 1194.1 and Appendices A, B, and C, and are available at https://www.access-board.gov/ict/. Information about Section 508 is available at https://www.hhs.gov/web/section-508/index.html.

(b) Additional Section 508 accessibility standards applicable to this contract or order are identified as follows:

205 WCAG 2.0 Level A & AA Success Criteria 302

Functional Performance Criteria

502 Inoperability with Assistive Technology

503 Applications

504 Authoring Tools

602 Support Documentation

603 Support Services

If it is determined by the Government that ICT supplies, products, platforms, information, documentation, and services support provided by the Contractor do not conform to the described accessibility standards in the contract, remediation of the supplies, products, platforms, information, documentation, or services support to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(c) In the event of a modification(s) to this contract or order, which adds new ICT supplies or services or revises the type of, or specifications for, supplies, products, platforms, information, documentation, or services support, the Contracting Officer shall require that the Contractor submit a completed HHS Section 508 Accessibility Conformance Checklist (see *https://www.hhs.gov/web/section-508/accessibility-checklists/index.html*) or an Accessibility Conformance Report (ACR) (based on the

Voluntary Product Accessibility Template (VPAT) see https://www.itic.org/policy/accessibility/vpat), and any other additional information necessary to assist the Government in determining that the ICT supplies or services conform to Section 508 accessibility standards. If it is determined by the Government that ICT supplies, products, platforms, information, documentation, and services support provided by the Contractor do not conform to the described accessibility standards in the contract, remediation of the supplies, products, platforms, information, documentation, or services support to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(d) If this is an Indefinite-Delivery type contract, a Blanket Purchase Agreement or a Basic Ordering Agreement, the task/delivery order requests that include ICT supplies, products, platforms, information, documentation, or services support will define the specifications and accessibility standards for the order. In those cases, the Contractor shall be required to provide a completed HHS Section 508 Accessibility Conformance Checklist (see *https://www.hhs.gov/web/section-508/accessibility-checklists/index.html*) or an ACR (based on the VPAT see https://www.itic.org/policy/accessibility/vpat), and any other additional information necessary to assist the Government in determining that the ICT supplies, products, platforms, information, documentation, or services support conform to Section 508 accessibility standards. If it is determined by the Government that ICT supplies and services provided by the Contractor do not conform to the described accessibility standards in the provided documentation, remediation of the supplies, products, platforms, information, documentation, or services support to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(e) The contractor shall identify to the Contracting Officer any perceived exception or exemption to Section 508 requirements for review by the agency Section 508 Program.

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 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 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
503 Applications
504 Authoring Tools
602 Support Documentation
603 Support Services

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 details, whether they conform to a specific Section 508 accessibility standard, and any ongoing 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.

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 an offeror claims its supplies or services meet applicable Section 508 accessibility standards. It is later determined by the Government, i.e., after the 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. Checklists 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.

Period of Performance

August 18, 2026 through August 17, 2031
Year 1: 8/18/2026-8/17/2027
Year 2: 8/18/2027-8/17/2028
Year 3: 8/18/2028-8/17/2029
Year 4: 8/18/2029-8/17/2030
Year 5: 8/18/2030-8/17/2031

C.7 Government Furnished Property

NA

C.8 References –

NA

Deliverables –

Delivery of the product will begin at the completion of the purchase.