SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

NOTE: OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, AND 30.

1. REQUISITION NUMBER

2. CONTRACT NUMBER

3. AWARD/EFFECTIVE DATE

4. ORDER NUMBER

5. SOLICITATION NUMBER
75N98026Q00992

6. SOLICITATION ISSUE DATE
08/07/2026

7. FOR SOLICITATION INFORMATION CALL:

a. NAME
JACOB BALENSON

b. TELEPHONE NUMBER *(No collect calls)*
+1 301 827 8302

8. OFFER DUE DATE/ LOCAL TIME
08/27/2026 1400 ES

9. ISSUED BY CODE OD/OALM

National Institutes of Health
Div. Simplified Acq. Policy & Services, OALM
6701 Rockledge Drive, RK II, 4th floor
Bethesda, MD 20817

10. THIS ACQUISITION IS [X] UNRESTRICTED OR [ ] SET ASIDE: % FOR:

[ ] SMALL BUSINESS
[ ] HUBZONE SMALL BUSINESS
[ ] SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS (SDVOSB)
[ ] WOMEN-OWNED SMALL BUSINESS (WOSB)
[ ] ECONOMICALLY DISADVANTAGED WOMEN-OWNED SMALL BUSINESS (EDWOSB)
[ ] 8(A)

NORTH AMERICAN INDUSTRY CLASSIFICATION STANDARD (NAICS): 513120

SIZE STANDARD: 1,000

11. DELIVERY FOR FREE ON BOARD (FOB) DESTINATION UNLESS BLOCK IS MARKED
[X] SEE SCHEDULE

12. DISCOUNT TERMS

[ ] 13a. THIS CONTRACT IS A RATED ORDER UNDER THE DEFENSE PRIORITIES AND ALLOCATIONS SYSTEM - DPAS (15 CFR 700)

13b. RATING

14. METHOD OF SOLICITATION
[X] REQUEST FOR QUOTE (RFQ) [ ] INVITATION FOR BID (IFB) [ ] REQUEST FOR PROPOSAL (RFP)

15. DELIVER TO CODE
See Schedule

16. ADMINISTERED BY CODE OD/OALM
See Schedule

17a. CONTRACTOR/ OFFEROR CODE FACILITY CODE

TELEPHONE NUMBER

[ ] 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

18a. PAYMENT WILL BE MADE BY CODE

18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED [ ] SEE ADDENDUM

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	ADMINISTERED BY: National Institutes of Health OALM/OLAO/SSIT 6701 Rockledge Drive, RK II, 5th floor Bethesda MD 20817 Continued... *(Use Reverse and/or Attach Additional Sheets as Necessary)*				

25. ACCOUNTING AND APPROPRIATION DATA

26. TOTAL AWARD AMOUNT *(For Government Use Only)*

[ ] 27a. SOLICITATION INCORPORATES BY REFERENCE (FEDERAL ACQUISITION REGULATION) FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA [ ] ARE [ ] ARE NOT ATTACHED

[ ] 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA [ ] ARE [ ] ARE NOT ATTACHED

[ ] 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN _____ COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED

[ ] 29. AWARD OF CONTRACT: REFERENCE _____ OFFER DATED. _____. YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR

31a. UNITED STATES OF AMERICA *(SIGNATURE OF CONTRACTING OFFICER)*

30b. NAME AND TITLE OF SIGNER *(Type or print)*

30c. DATE SIGNED

31b. NAME OF CONTRACTING OFFICER *(Type or print)*
SHIRLEY RUIZ-LUNDGREN

31c. DATE SIGNED

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
1	The Contractor shall provide a fully integrated journal submission, manuscript review, and web publishing/hosting platform solution for the Journal of Replication and Reproducibility (JRR) Product/Service Code: 7630 Product/Service Description: NEWSPAPERS AND PERIODICALS Period of Performance: 09/28/2026 to 09/27/2027				

32a. QUANTITY IN COLUMN 21 HAS BEEN

☐ RECEIVED ☐ INSPECTED ☐ ACCEPTED, AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED: _____

32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32c. DATE	32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE 32g. EMAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE

33. SHIP NUMBER ☐ PARTIAL ☐ FINAL	34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT ☐ COMPLETE ☐ PARTIAL ☐ FINAL	37. CHECK NUMBER

STOCK RECORD (S/R)		40. PAID BY
38. S/R ACCOUNT NUMBER	39. S/R VOUCHER NUMBER	

41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT		42a. RECEIVED BY *(Print)*	
41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER	41c. DATE	42b. RECEIVED AT *(Location)*	
		42c. DATE RECEIVED *(MM/DD/YYYY)*	42d. TOTAL CONTAINERS

SECTION B – SUPPLIES OR SERVICES AND PRICES/COSTS

ARTICLE B.1. BRIEF DESCRIPTION OF SUPPLIES OR SERVICES

The Contractor shall provide a fully integrated journal submission, manuscript review, and web publishing/hosting platform solution for the Journal of Replication and Reproducibility (JRR), including web hosting, submission and open peer review, preprint and final publication, single-source XML publishing, code repositories, containerized compute, continuous publication, and related platform support services in accordance with the Performance Work Statement (PWS).

ARTICLE B.2. PRICES/COSTS

a. This is a Firm-Fixed-Price (FFP) type purchase order. The Contractor will be paid the firm-fixed price established at award for successful performance of the requirements of the contract.

b. Upon performance and Government acceptance of the services and deliverables required by Attachment 1 - Performance Work Statement (PWS) and Attachment 1A – Deliverables, the Government will pay the Contractor in accordance with the pricing schedule set forth below and in accordance with the invoicing terms of the contract:

SCHEDULE OF CHARGES FOR BASE PERIOD: 09/28/2026 – 09/27/2027 (Estimated)

CLIN	FIRM-FIXED PRICE
TBD	
TBD	
TBD	
TBD	
TBD	
TOTAL	

(END OF SECTION B)

SECTION C – TECHNICAL REQUIREMENTS

ARTICLE C.1. DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

Independently and not as an agent of the Government, the Contractor shall furnish all services, qualified personnel, supplies, equipment, and other resources necessary to perform the requirements of Attachment 1 – Performance Work Statement (PWS), which is incorporated into and made part of this contract.

ARTICLE C.2. REPORTING REQUIREMENTS/DELIVERABLES

The Contractor shall provide all reports, plans, data, and other deliverables required by Attachment 1 – Performance Work Statement (PWS), including Section 3.2, and Attachment 1A – Deliverables. All applicable submission requirements, frequencies, due dates, performance standards, acceptable quality levels (AQLs), and monitoring methods identified in those attachments are incorporated herein by reference. Unless otherwise directed by the Government, all electronic reports, documents, and other final deliverables shall comply with applicable Section 508 accessibility requirements.

(END OF SECTION C)

SECTION D – PACKAGING AND MARKING

ARTICLE D.1. PACKING, PACKAGING, AND MARKING

All deliverables under this contract shall be provided electronically unless otherwise directed by the Government. Electronic deliverables shall be clearly identified with the contract number, Contractor name, deliverable title, and submission date, as applicable. All deliverables shall be submitted in a complete, usable, and accessible format consistent with the requirements of the contract.

Any data or materials delivered with asserted restrictions on the Government's use, reproduction, disclosure, or distribution shall be appropriately marked at the time of delivery with the applicable restrictive legend or notice, consistent with PWS Section 8 – Data Rights and the applicable contract clauses.

(END OF SECTION D)

SECTION E - INSPECTION AND ACCEPTANCE

E.1. INSPECTION AND ACCEPTANCE

The Contracting Officer's Representative (COR), or other authorized Government representative as delegated, will perform inspection and acceptance of the services and deliverables provided under the contract in accordance with the Performance Work Statement (PWS) and the terms and conditions of the contract.

E.2. BASIS OF ACCEPTANCE

a. Acceptance will be based on compliance with the requirements, performance standards, and monitoring methods, as applicable, identified in the PWS, the Contractor's quotation as incorporated into the contract, and all other applicable terms and conditions of the contract.

b. Reports, documents, and other deliverables will be accepted when they satisfy the applicable contract requirements and any discrepancies, errors, or deficiencies identified by the Government have been satisfactorily corrected.

(END OF SECTION E)

SECTION F – DELIVERIES OR PERFORMANCE

ARTICLE F.1. PERIOD OF PERFORMANCE

Estimated Period of Performance: September 28, 2026 through September 27, 2027.

ARTICLE F.2. PLACE OF PERFORMANCE

The Contractor shall perform the services at Contractor-provided facilities or other Contractor-controlled locations within the continental United States, in accordance with the PWS.

ARTICLE F.3. NOTICE TO THE GOVERNMENT OF DELAYS

In the event the Contractor encounters difficulty in meeting performance requirements or anticipates difficulty in complying with any contract delivery schedule or completion date, or becomes aware of any actual or potential situation that is delaying or threatens to delay timely performance, the Contractor shall immediately notify the Contracting Officer (CO) and Contracting Officer's Representative (COR) in writing. The notification shall provide pertinent details regarding the delay, its anticipated impact, and any proposed corrective or mitigation actions. Such notification is for informational purposes only and shall not constitute a waiver of any contract requirement, delivery schedule, or Government right or remedy.

(END OF SECTION F)

SECTION G – CONTRACT ADMINISTRATION DATA

ARTICLE G.1. CONTRACTING OFFICER REPRESENTATIVE (COR)

The following Contracting Officer's Representative (COR) will represent the Government for the purpose of this contract:

TBD - To be designated at award.

The Contracting Officer's Representative is responsible for: (1) monitoring the Contractor's technical progress, including the surveillance and assessment of performance and recommending to the Contracting Officer changes in requirements; (2) interpreting the Performance Work Statement (PWS) and any other technical performance requirements; (3) performing technical evaluation as required; (4) performing technical inspections and acceptances required by this contract; and (5) assisting in the resolution of technical problems encountered during performance..

The Contracting Officer is the only person with authority to act as agent of the Government under this contract. Only the Contracting Officer has authority to: (1) direct or negotiate any changes in the PWS; (2) modify or extend the period of performance; (3) change the delivery schedule; (4) authorize reimbursement to the Contractor for any costs incurred during the performance of this contract; or (5) unilaterally change its COR designation.

ARTICLE G.2. KEY PERSONNEL, HHSAR 352.237-75 (DECEMBER 2015)

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

(End of Clause)

Additional Key Personnel Requirements

b. In the event that any Key Personnel named in the contract are unable to perform because of death, illness, resignation from the Contractor's employment, dissolution of agreement, or other reasons, the Contractor shall submit to the Contracting Officer within **five (5) business days** a detailed written explanation of the circumstances necessitating the proposed substitution, complete resumes/CVs for the proposed substitute(s), and any other information the Contracting Officer deems pertinent to evaluate the proposed substitution. No substitution shall be made without the prior written approval of the Contracting Officer. No increase in contract price will be allowed as a result of a Government-approved substitution.

c. The Contracting Officer reserves the right to require removal of any Contractor employee performing under the contract who is determined not to possess the appropriate level of competence or ability, or who is

otherwise determined to be unsuitable for the work required. In such cases, the Contractor shall promptly submit the name and qualifications of a proposed replacement and any other information, as requested by the Contracting Officer.

d. Failure or delay by the Contractor in providing qualified personnel who meet the requirements of the contract may constitute a failure to comply with the terms and conditions of the contract and may be grounds for termination for cause in accordance with RFO FAR 52.212-4.

The following individual(s) is/are considered to be essential to the work being performed hereunder:

NAME	TITLE
TBD	TBD
TBD	TBD

ARTICLE G.3. INVOICE SUBMISSION

a. The Contractor must submit invoices to the Department of Treasury's Invoice Processing Platform (IPP) at https://www.ipp.gov, with a copy to the approving official for approval, as directed below and in accordance with the definitions of timeliness set forth in the invoice instructions included as an attachment in Section J of this Contract.

b. The contractor's failure to submit timely invoice(s) to the Government waives the contractor's rights to receive payment pursuant to this contract. In the event of this waiver, the Government is not obligated to make such payment, and the Contracting Officer shall have the authority to unilaterally deobligate the funds in accordance with the requirements at 31 U.S.C. 1552(a) and downwardly adjust the total amount of the award by the amount of the deobligation. The contractor shall be given an opportunity to request the excusal of a late invoice from the Contracting Officer. If excused, the Contracting Officer will respond in writing to confirm that the contactor's right to receive payment has not been waived.

c. Payment requests (invoices) shall be submitted in accordance with HHSAR 352.232-71 Electronic Submission of Payment Requests (DEVIATION APR 2026). In addition, Contractor shall submit an electronic copy of the payment request (invoice) to the approving official instead of a paper copy. The payment request (invoice) shall be transmitted as an attachment via e-mail to the addresses listed below in one of the following formats: MSWord, MS Excel, or Adobe Portable Document Format (PDF). Only one payment request shall be submitted per e-mail, and the subject line of the e-mail shall include the Contractor's name, contract number, and unique invoice number.

OALM SSIT Contractor Submissions Central Mailbox (oalm-ssit-contractor@mail.nih.gov)
• Contracting Officer: Shirley Ruiz-Lundgren, shirley.ruiz-lundgren@nih.gov
• Contract Specialist: Jacob Balenson, jacob.balenson@nih.gov

Questions concerning the transition to IPP should be directed to NIH-IPPinvoicing@mail.nih.gov. Questions concerning this award should be directed to the Contract Specialist and/or Contracting Officer.

ARTICLE G.4. PROVIDING ACCELERATED PAYMENT TO SMALL BUSINESS SUBCONTRACTORS, RFO 52.232-40 (MAR 2023)

(a) (1) In accordance with 31 U.S.C. 3903 and 10 U.S.C. 3801, within **15 days** after receipt of accelerated payments from the Government, the Contractor shall make accelerated payments to its small business subcontractors under this contract, to the maximum extent practicable and prior to when such payment is

otherwise required under the applicable contract or subcontract, after receipt of a proper invoice and all other required documentation from the small business subcontractor.

(2) The Contractor agrees to make such payments to its small business subcontractors without any further consideration from or fees charged to the subcontractor.

(b) The acceleration of payments under this clause does not provide any new rights under the Prompt Payment Act.

(c) Include the substance of this clause, including this paragraph (c), in all subcontracts with small business concerns, including subcontracts with small business concerns for the acquisition of commercial products or commercial services.

(End of clause)

ARTICLE G.5. POST AWARD EVALUATION OF CONTRACTOR PERFORMANCE)

a. Contractor Performance Evaluations: Interim and Final Evaluations of Contractor performance will be prepared on this contract in accordance with RFO FAR Subpart 42.11 - Contractor Performance Information. The final performance evaluation will be prepared at the time of completion of work. In addition to the final evaluation, interim evaluation(s) will be prepared on the annual anniversary dates of the contract. Interim and Final evaluations will be provided to the Contractor as soon as practicable after completion of the evaluation. The Contractor will be permitted **14 calendar days** to review the document and to submit additional information or a rebutting statement. If agreement cannot be reached between the parties, the matter will be referred to an individual one level above the Contracting Officer, whose decision will be final. Copies of the evaluations, Contractor responses, and review comments, if any, will be retained as part of the contract file, and may be used to support future award decisions.

b. Electronic Access to Contractor Performance Evaluations: Contractors may access evaluations through a secure Web site for review and comment at the following address: http://www.cpars.gov.

(END OF SECTION G)

SECTION H – SPECIAL CONTRACT REQUIREMENTS

ARTICLE H.1. DISSEMINATION OF FALSE OR DELIBERATELY MISLEADING INFORMATION

The Contractor shall not use contract funds to disseminate information that is deliberately false or misleading.

ARTICLE H.2. RESTRICTION OF PORNOGRAPHY ON COMPUTER NETWORKS

The Contractor shall not use contract funds to maintain or establish a computer network unless such network blocks the viewing, downloading, and exchanging of pornography.

ARTICLE H.3. GUN CONTROL

The Contractor shall not use contract funds in whole or in part, to advocate or promote gun control.

ARTICLE H.4. INFORMATION SECURITY AND/OR PHYSICAL ACCESS SECURITY REQUIREMENTS

SECTION A – BASELINE SECURITY REQUIREMENTS

1. 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:
   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 HHS mission. In addition to the Revolutionary FAR Overhaul (RFO) 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/NIH policies and level of risk. At a minimum, the Contractor (and/or any subcontractor) must:
   i. Protect the:
      - **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 HHS/NIH and information systems that store, process, and/or transmit HHS 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 NIH/OD ISSO or other designated NIH security/privacy representative, NIH/OD SOP, 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:** [ ] Low [**X**] Moderate [ ] High
- **Integrity:** [ ] Low [**X**] Moderate [ ] High
- **Availability:** [ ] Low [**X**] Moderate [ ] High
- **Overall Impact Level:** [ ] Low [**X**] 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 HHS/NIH 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 HHS/NIH 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 HHS/NIH security and/or privacy officials.

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

d. **Privacy Compliance.** Comply with the E-Government Act of 2002, NIST SP 800-53, and applicable HHS/NIH/OD 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. Based on information provided by the ISSO, system/data owner, or other security or privacy representative, it has been determined that this solicitation/contract involves:

[ ] No PII [**X**] 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 or not a full Privacy Impact Assessment (PIA) needs to be completed.
111

- 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 **60 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*.
- 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.

e. **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 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*.

f. **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.

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

h. **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)*.

i. **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, RFO FAR 40.204-2, RFO FAR 52.240-90, and RFO FAR 52.240-91. 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.

j. **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 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, HTTPS is not required, but it is highly recommended. Consult the *HHS Policy for Internet and Email Security* for additional information.

k. **Contract Documentation***.* The Contractor must use provided templates, policies, forms and other agency documents. NIH will specify which documents/forms will be provided to comply with contract deliverables as appropriate.

l. **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 HHS and NIH-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 within **15 days** of the validation.
   v. 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 http://csrc.nist.gov/publications/. Encryption keys must be provided to the COR upon request and at the conclusion of the contract.

m. **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 NIH/OD non-disclosure agreement, https://ocio.nih.gov/aboutus/publicinfosecurity/acquisition/Documents/Nondisclosure.pdf , 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 HHS/NIH/OD 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 https://irtsectraining.nih.gov/ Information Security Awareness, Privacy, and Records Management training at least ***annually***, during the life of this contract. All provided training must be compliant with HHS 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 policy and the *HHS Role-Based Training (RBT) of Personnel with Significant Security Responsibilities Memorandum*. Read further guidance about the NIH Role-based Training at: https://www.hhs.gov/about/agencies/asa/ocio/cybersecurity/security-awareness-training/index.html .

c. **Training Records.** The Contractor (and/or any subcontractor) must maintain training records for all its employees working under this contract in accordance with HHS 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 *HHS Information Technology General Rules of Behavior*, *HHS Rules of Behavior for Privileged Users*.
b. 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 NIH 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 HHS Computer Security Incident Response Center (CSIRC)/NIH IRT teams **within 24 hours,** whether the response is positive or negative.

   FISMA defines an incident as "an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. In accordance with OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information (PII)*, 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 HHS breach response process, please see the *HHS Policy and Plan for Preparing for and Responding to a Breach of Personally Identifiable Information (PII)*."

b. In the event of a suspected or confirmed incident or breach, the Contractor (and/or any subcontractor) must:
   i. Protect all sensitive information, including any PII created, stored, or transmitted in the performance of this contract, with encryption solution that is validated with current FIPS 140 validation certificate from the NIST CMVP.
   ii. 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 must send NIH approved notifications to affected individuals in accordance with https://wiki.ocio.nih.gov/wiki/index.php/US-CERT_Federal_Incident_Notification_Guidelines .
   iii. Report all suspected and confirmed information security and privacy incidents and breaches to the NIH Information Security Program contact team via e-mail at NIHInfoSec@nih.gov, NIH Incident Response Team (IRT) via email at IRT@mail.nih.gov , COR, CO, NIH/OD SOP (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 NIH/OD 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, 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.

iv. Comply with OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information,* and HHS/NIH and NIH privacy breach response policies when handling PII breaches.

v. 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 within an **hour** of discovery.

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:

[ ] Tier 5: Critical Sensitive and Special Sensitive National Security, including Top Secret, SCI, and "Q" access eligibility.
[ ] Tier 5SR: Reinvestigation.

[ ] Tier 4: High Risk Public Trust (HRPT).
[ ] Tier 4SR: Reinvestigation.

[ ] Tier 3: Non-Critical Sensitive, National Security, including Secret and "L" access eligibility.
[ ] Tier 3SR: Reinvestigation.

[X] Tier 2: Non-Sensitive / Moderate Risk (Public Trust).
[ ] Tier 2S with Subject Interview: Moderate Risk Public Trust (MRPT).
[ ] Tier 2SR: Reinvestigation.

[ ] Tier 1: Low Risk, Non-Sensitive, including HSPD-12 Credentialing.

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 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

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 within **seven (7) calendar days** of the effective date of this contract. Any revisions to the roster as a result of staffing changes must be submitted within **seven**

(7) calendar days of the change. The COR will notify the Contractor of the appropriate level of investigation required for each staff member. An electronic template, "Roster of Employees Requiring Suitability Investigations," is available for Contractor use at: - https://oamp.od.nih.gov/nih-document-generation-system/dgs-workform-information/attachment-files-section-j
If the employee is filling a new position, the Contractor must provide a position description and the Government will determine the appropriate suitability level. Upon receipt of the Government's notification of applicable Suitability Investigations required, the Contractor shall complete and submit the required forms within **30 days** of the notification.

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, 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 must follow the HHS EPLC framework and methodology and in accordance with the HHS Contract Closeout Directive (2018) located at: https://oamp.od.nih.gov/sites/default/files/DGS/contracting-forms/HHS-Closeout-Directive-2018.pdf . HHS EA requirements are located at: https://www.hhs.gov/web/governance/digital-strategy/it-policy-archive/hhs-policy-for-enterprise-architecture.html and NIH EA requirements are located at: https://ocio.nih.gov/it-governance/managing-it-projects-and-investments .
b. **System Documentation.** Contractors (and/or any subcontractors) must follow and adhere to HHS 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 in accordance with the NIH Media Sanitization and Disposal Policy 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 ISSO within **fifteen days** 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 NIH policies.
f. The Contractor (and/or any subcontractor) must perform and document the actions identified in the NIH Employee Separation Checklist https://ocio.nih.gov/sites/external/files/2024-01/Emp-sep-checklist.pdf when an employee terminates work under this contract within **2 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 *HHS Policy for Records Management* and NIH policies and must not dispose of any records unless authorized by HHS/ NIH.

b. In the event that 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 HHS/NIH policies.

10. High Value Asset (HVA)

If a system is identified as HVA,[23] the Contractor must comply with the HHS Policy for the High Value Asset (HVA) Program and the DHS HVA Control Overlay[24] in addition to the above requirements.

SECTION B - GOVERNMENT INFORMATION PROCESSED ON GOCO OR COCO SYSTEMS

1. SECURITY REQUIREMENTS FOR GOVERNMENT-OWNED/CONTRACTOR-OPERATED (GOCO) AND CONTRACTOR-OWNED/CONTRACTOR-OPERATED (COCO) RESOURCES

a. **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); National Institutes of Health (NIH) Information Security (InfoSec) Policy Handbook; 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.

b. **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:

i. 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.

ii. 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.

- 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.

- Cooperate with inspections, audits, investigations, and reviews.

c. **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.

d. **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:

   i. Encrypt equipment and sensitive information stored and/or processed by such equipment in accordance with HHS and FIPS 140-3 encryption standards.
   ii. Configure laptops and desktops in accordance with the latest applicable United States Government Configuration Baseline (USGCB), and HHS Minimum Security Configuration Standards;
   iii. Maintain the latest operating system patch release and anti-virus software definitions within **15 days**.
   iv. 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
   v. 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.

e. **Rights to Data.** All contracts that require data to be produced, furnished, acquired, or used in meeting contract performance requirements, must contain terms that delineate the respective rights and obligations of the Government and the contractor regarding the use, reproduction, and disclosure of that data. Data rights clauses do not specify the type, quantity or quality of data that is to be delivered, but only the respective rights of the Government and the contractor regarding the use, disclosure, or reproduction of the data. Accordingly, the contract must specify the data to be delivered.

f. **Information and Communications Technology (ICT) Cybersecurity Supply Chain Risk Management (C-SCRM) requirements**. The Contractor (and/or any subcontractor) must secure their ICT supply chain in compliance with *HHS Policy for Cyber Supply Chain Risk Management* and Public Law 115-232 § 889. At a minimum, they must implement the following:
   i. Develop rules for suppliers' development methods, techniques, or practices;
   ii. Use of secondary market components;
   iii. Prohibit counterfeit products;
   iv. Dispose and/or retain elements such as components, data, or intellectual property securely;
   v. Ensure adequate supply of components;
   vi. Require external providers handling federal information or operating systems on behalf of the federal government to meet the same security and privacy requirements as federal agencies;
   vii. Require external providers to express security and privacy requirements (including the controls for systems processing, storing, or transmitting federal information) in contracts or other formal agreements;
   viii. Establish Service Level Agreements (SLAs), patching vehicles and disclosure requirements in the case of a security incident or new vulnerability being discovered; and
   ix. Ensure that the supplier applies same contractual requirements to any sub-contractors/suppliers that they involve in the provision of the product or service to the customer; and
   x. Prohibit the use of covered telecommunications and video surveillance equipment or services.

SECTION C - NON-COMMERCIAL AND OPEN-SOURCE COMPUTER SOFTWARE PROCUREMENTS

1. The Contractor (and/or any subcontractor) must follow secure coding best practice requirements, as directed by the 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. The Contractor will be liable for malicious or defective code or failure to reduce risk.

SECTION D - INFORMATION TECHNOLOGY APPLICATION DESIGN, DEVELOPMENT, OR SUPPORT

a. The Contractor (and/or any subcontractor) must ensure IT applications designed and developed for end users (including mobile applications and software licenses) run in the standard user context without requiring elevated administrative privileges.
b. The Contractor (and/or any subcontractor) must 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.
c. The Contractor (and/or any subcontractor) must ensure that computer software developed on behalf of HHS or tailored from an open-source product, is fully functional and operates correctly on systems configured in accordance with government policy and federal configuration standards. The contractor must test applicable products and versions with all relevant and current updates and patches updated prior to installing in the HHS environment. No sensitive data must be used during software testing.
d. The Contractor (and/or any subcontractor) must protect information that is deemed sensitive from unauthorized disclosure to persons, organizations or subcontractors who do not have a need to know the information. Information which, either alone or when compared with other reasonably-available information, is deemed sensitive or proprietary by HHS must be protected as instructed in accordance with the magnitude of the loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. This language also applies to all subcontractors that are performing under this contract.

ARTICLE H.5. REPORTING MATTERS INVOLVING FRAUD, WASTE AND ABUSE

Anyone who becomes aware of the existence or apparent existence of fraud, waste and abuse in NIH funded programs is encouraged to report such matters to the HHS Inspector General's Office in writing or on the Inspector General's Hotline. The toll free number is **1-800-HHS-TIPS (1-800-447-8477).** All telephone calls will be handled confidentially. The website to file a complaint on-line is: http://oig.hhs.gov/fraud/hotline/ and the mailing address is:

US Department of Health and Human Services
Office of Inspector General
ATTN: OIG HOTLINE OPERATIONS
P.O. Box 23489
Washington, D.C. 20026

ARTICLE H.6. CONTRACTOR PERSONNEL

The Contractor shall be responsible for managing and overseeing the activities of all Contractor personnel, as well as subcontractor efforts used in performance of this effort. The Contractor's management responsibilities shall include all activities necessary to ensure the accomplishment of timely and effective support, performed in accordance with the requirements contained in the Performance Work Statement (PWS). Resumes submitted for employees assigned to perform under this PWS shall contain documented experience directly applicable to the functions to be performed. Further, these prior work experiences shall be specific and of sufficient variety and duration that the employee is able to effectively and efficiently perform the functions assigned.

The Contractor shall identify the personnel responsible for management and coordination of contract performance and shall provide appropriate points of contact to the Contracting Officer and COR. Contractor personnel shall meet the applicable qualifications and expertise requirements identified in the PWS.

ARTICLE H.7. NON-PERSONAL SERVICES AND INHERENTLY GOVERNMENTAL FUNCTIONS

Pursuant to RFO FAR Subpart 37.2, no personal services shall be performed under this award. All work requirements shall flow only from the COR to the Contractor’s designated management point of contact. No Contractor employee will be directly supervised by the Government. All individual employee assignments, and daily work direction, shall be given by the applicable contractor supervisor. If the Contractor 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 will promptly notify the CO of this communication or action.

Pursuant to RFO 7.5, the Contractor shall not perform any inherently governmental actions under this award. 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 award, Contractor employees shall identify themselves as Contractor employees and/or consultants specify the name of the company for which they are employed. In all communications with other Government contractors in connection with this contract, the Contractor employee will state that they have no authority to in any way change the contract and that if the other contractor believes this communication to be a direction to change their contract, they should notify the CO for that contract and not carry out the direction until a clarification has been issued by the CO.

The Contractor shall ensure that all of its employees working in this award are informed of the substance of this section. Nothing in this section shall limit the Government’s rights in any way under the provisions of this

award, including those related to the Government's right to inspect and accept the service to be performed under this award. The substance of this article shall be included in all subcontracts at any tier.

ARTICLE H.9. CONFIDENTIALITY AND DISCLOSURE INFORMATION

Information made available to the Contractor by the Government for the performance or administration of this effort shall be used only for those purposes and shall not be used in any other way without the written agreement of the Contracting Officer.

The Contractor agrees to assume responsibility for protecting the confidentiality of Government records, which are not public information. Each contractor or employee of the Contractor to whom information may be made available or disclosed shall be notified in writing by the Contractor that such information may be disclosed only for a purpose and to the extent authorized herein.

ARTICLE H.10. GOVERNMENT FURNISHED PROPERTY

No Government-furnished property is anticipated to be provided under this contract. The Contractor shall furnish all supplies, equipment, hardware, software, licenses, internet access, and services necessary to perform the requirements of the PWS.

ARTICLE H.11. INFORMATION REGARDING SECTION 508

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use information and communication technology (ICT), it shall be accessible to people with disabilities. Federal employees and members of the public who have disabilities must have access to, and use of, information and data that is comparable to people without disabilities.

Products, platforms and services delivered as part of this work statement that are ICT, or contain ICT, must conform to the Revised 508 Standards, which are located at 36 C.F.R. § 1194.1 & Apps. A, C & D, and available at https://www.access-board.gov/ict/.

Applicable Functional Performance Criteria: All functional performance criteria apply when using an alternative design or technology that achieves substantially equivalent or greater accessibility and usability by individuals with disabilities, than would be provided by conformance to one or more of the requirements in Chapters 4-6 of the Revised 508 Standards, or when Chapters 4-6 do not address one or more functions of ICT.

Applicable requirements for software features and components: All WCAG Level AA Success Criteria, 502 Interoperability with Assistive Technology, 503 Application.

Applicable requirements for hardware features and components: All requirements apply Applicable support services and documentation: All requirements apply Prior to acceptance, the government reserves the right to perform testing on required ICT items to validate the offeror's Section 508 conformance claims. If the government determines that Section 508 conformance claims provided by the offeror represent a higher level of conformance than what is actually provided to the agency, the government shall, at its option, require the offeror to remediate the item to align with the offeror's original Section 508 conformance claims prior to acceptance.

The law (29 U.S.C § 794 (d)) applies to all Federal agencies when they develop, procure, maintain, or use electronic and information technology. Responses to this solicitation shall be compliant with Section 508

(https://www.hhs.gov/web/section-508/accessibility-checklists/index.html). The Contractor shall comply with Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d) for this solicitation. Knowledge of Section 508 requirements and ways to remediate problems identified is required of the Contractor. Familiarity with the hardware and software used by people with disabilities is desirable. Pursuant to Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d) (Rehabilitation Act Amendments of 1998) all Electronic and Information Technology (EIT) developed, procured, maintained and/or used under this SOW shall be in compliance with the “Electronic and Information Technology Accessibility Standards” set forth by the Architectural and Transportation Barriers Compliance Board (also referred to as the “Access Board”) in 36 CFR Part 1194. The complete text of Section 508 Final Standards can be accessed at http://www.access-board.gov.

In addition to the applicable Revised 508 Standards, all content published in JRR shall conform to WCAG 2.2 Level AA as required by the PWS.

(END OF SECTION H)

SECTION I CONTRACT CLAUSES

ARTICLE I.1. REVOLUTIONARY FAR OVERHAUL (RFO) FEDERAL ACQUSITION REGULATIONS (FAR)

This Contract incorporates the following additional Revolutionary FAR Overhaul (RFO) clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer shall make the full text available. In addition, the full text of a RFO clause may be accessed electronically at www.acquisition.gov. (RFO FAR deviation text is available at https://www.acquisition.gov/far-overhaul).

- RFO FAR 52.203-6, Restrictions on Subcontractor Sales to the Government (JUN 2020), Alternate I (NOV 2021)
- RFO FAR 52.203-11, Certification and Disclosure Regarding Payments to Influence Certain Federal Transactions (SEP 2024)
- RFO FAR 52.203-17, Contractor Employee Whistleblower Rights (NOV 2023)
- RFO FAR 52.203-18, Prohibition on Contracting with Entities that Require Certain Internal Confidentiality Agreements or Statements—Representation (JAN 2017)
- RFO FAR 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (JAN 2017)
- RFO FAR 52.204-7, System for Award Management (AUG 2025)
- RFO FAR 52.204-13, System for Award Management—Maintenance (AUG 2025)
- RFO FAR 52.204-19, Incorporation by Reference of Representations and Certifications (DEC 2014)
- RFO FAR 52.209-2, Prohibition on Contracting with Inverted Domestic Corporations-Representation (AUG 2025)
- RFO FAR 52.209-5, Certification Regarding Responsibility Matters
- RFO FAR 52.209-6, Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, Proposed for Debarment, or Voluntarily Excluded (AUG 2025)
- RFO FAR 52.209-9, Updates of Publicly Available Information Regarding Responsibility Matters (OCT 2018)
- RFO FAR 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations
- RFO FAR 52.209-11, Representation by Corporations, Regarding Delinquent Tax Liability or a Felony Conviction under any Federal Law
- RFO FAR 52.212-1, Instructions to Offerors—Commercial Products and Commercial Services (AUG 2025)
- RFO FAR 52.212-2, Evaluation-Commercial Products and Commercial Services (AUG 2025)
- RFO FAR 52.212-4, Contract Terms and Conditions – Commercial Products and Commercial Services (AUG 2025)
- RFO FAR 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (OCT 2022).
- RFO FAR 52.219-8, Utilization of Small Business Concerns (SEP 2025)
- RFO FAR 52.219-9, Small Business Subcontracting Plan
- RFO FAR 52.219-16, Liquidated Damages—Subcontracting Plan (SEP 2025)
- RFO FAR 52.219-28, Postaward Small Business Program Rerepresentation (JAN 2025)
- RFO FAR 52.222-3, Convict Labor (JUN 2003)
- RFO FAR 52.222-19, Child Labor—Cooperation with Authorities and Remedies (MAR 2026)
- RFO FAR 52.224-3, Privacy Training (JAN 2017)
- RFO FAR 52.232-25, Prompt Payment
- RFO FAR 52.232-33, Payment by Electronic Funds Transfer—System for Award Management (OCT 2018)
- RFO FAR 52.232-40, Providing Accelerated Payments to Small Business Subcontractors

- RFO FAR 52.233-3, Protest After Award (AUG 2025)
- RFO FAR 52.233-4, Applicable Law for Breach of Contract Claim (AUG 2025)
- RFO FAR 52.222-35, Equal Opportunity for Veterans (JUN 2020)
- RFO FAR 52.222-36, Equal Opportunity for Workers with Disabilities (JUN 2020)
- RFO FAR 52.222-37, Employment Reports on Veterans (JUN 2020)
- RFO FAR 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (DEC 2010)
- RFO FAR 52.222-50, Combating Trafficking in Persons (OCT 2025)
- RFO FAR 52.222-54, Employment Eligibility Verification (JAN 2025)
- RFO FAR 52.222-90, Addressing DEI Discrimination by Federal Contractors (APR 2026)
- RFO FAR 52.223-23, Sustainable Products and Services (MAY 2024)
- RFO FAR 52.226-8, Encouraging Contractor Policies to Ban Text Messaging While Driving (MAY 2024)
- RFO FAR 52.229-11, Tax on Certain Foreign Procurements—Notice and Representation (JUN 2020)
- RFO FAR 52.237-3, Continuity of Services (JAN 1991)
- RFO FAR 52.240-90, Security Prohibitions and Exclusions Representations and Certifications (AUG 2025)
- RFO FAR 52.240-91, Security Prohibitions and Exclusions (AUG 2025)
- RFO FAR 52.240-93, Basic Safeguarding of Covered Contractor Information Systems (AUG 2025)
- RFO FAR 52.242-5, Payments to Small Business Subcontractors (JAN 2017).
- RFO FAR 52.244-6, Subcontracts for Commercial Products and Commercial Services (SEP 2025)
- RFO FAR 52.252-1, Solicitation Provisions Incorporated by Reference (FEB 1998)
- RFO FAR 52.252-2, Clauses Incorporated by Reference (FEB 1998)
- RFO FAR 52.252-5, Authorized Deviations in Provisions (NOV 2020)
- RFO FAR 52.252-6, Authorized Deviations in Clauses (NOV 2020)

ARTICLE I.2. DEPARTMENT OF HEALTH AND HUMAN SERVICES ACQUISITION REGULATION (HHSAR)

This Contract incorporates the following Department of Health and Human Services Regulation (HHSAR) Clause by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make the respective clauses full text available. In addition, the full text of a HHSAR clause may be accessed electronically at: https://www.hhs.gov/grants/contracts/contract-policies-regulations/hhsar/index.html.

- HHSAR 352.204-72, Records Management (FEB 2024 DEVIATION)
- HHSAR 352.204-73, Contractor Personnel Security and Agency Access (FEB 2024 DEVIATION)
- HHSAR 352.224-70, Notification of System of Records Notice (FEB 2024 DEVIATION)
- HHSAR 352.224-71, Confidential Information (FEB 2024 DEVIATION)
- HHSAR 352.232-71, Electronic Submission of Payment Requests (APR 2026 DEVIATION)
- HHSAR 352.237-75, Key Personnel (DEC 2015)
- HHSAR 352.239-71, Security Requirements for Information Technology Resources (FEB 2024 DEVIATION)
- HHSAR 352.239-72, Information System Security Plan and Accreditation (FEB 2024 DEVIATION)
- HHSAR 352.239-73, Information System Design and Development (FEB 2024 DEVIATION)
- HHSAR 352.239-74, Information System Hosting, Operation, Maintenance, or Use (FEB 2024 DEVIATION)
- HHSAR 352.239-75, Security Controls Compliance Testing (FEB 2024 DEVIATION)

- HHSAR 352.239-76, Security Requirements for Government-Owned Contractor-Operated and Contractor-Owned Contractor-Operated Resources (FEB 2024 DEVIATION)
- HHSAR 352.239-77, Cloud Computing Services (FEB 2024 DEVIATION)
- HHSAR 352.239-78, Information and Communication Technology Accessibility Notice (FEB 2024 DEVIATION)
- HHSAR 352.239-79, Information and Communication Technology Accessibility (FEB 2024 DEVIATION)

(END OF SECTION I)

SECTION J – LIST OF ATTACHMENTS

The following documents are attached and incorporated in this contract:

- Attachment 1 – Performance Work Statement (PWS)
- Attachment 1A – Deliverables
- Attachment 2 - Quote Instructions and Evaluation Criteria
- Attachment 3 – HHSAR IT Clauses
- Attachment 4 – NIH Invoicing Instructions

(END OF SECTION J)

END OF CONTRACT