SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS

OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30

1. REQUISITION NUMBER

PAGE 1 OF 141

2. CONTRACT NO.

3. AWARD/ EFFECTIVE DATE

4. ORDER NUMBER

5. SOLICITATION NUMBER: 7571MN26Q00039

6. SOLICITATION ISSUE DATE: 07/07/2026

7. FOR SOLICITATION INFORMATION CALL:

a. NAME: CHRISTOPHER POULOS

b. TELEPHONE NUMBER *(No collect calls)*

8. OFFER DUE DATE/LOCAL TIME: 07/30/2026 1500 ET

9. ISSUED BY CODE OMAS-MN

OMAS Mission Support
5600 Fishers Lane
Rockville MD 20852

10. THIS ACQUISITION IS ☒ 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): 541611

SIZE STANDARD: $24.5

11. DELIVERY FOR FREE ON BOARD (FOB) DESTINATION UNLESS BLOCK IS MARKED
☒ 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
☒ REQUEST FOR QUOTE (RFQ) ☐ INVITATION FOR BID (IFB) ☐ REQUEST FOR PROPOSAL (RFP)

15. DELIVER TO CODE ACL

ACL
Administration for Community Living
330 C Street, SW; Room 1318A
Washington DC 20024

16. ADMINISTERED BY CODE OMAS-MN

OMAS Mission Support
5600 Fishers Lane
Rockville MD 20852

17a. CONTRACTOR/ OFFEROR CODE FACILITY CODE

TELEPHONE NO.

☐ 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
	Delivery: 09/30/2026 Period of Performance: 09/30/2026 to 09/29/2027				
1	Base University Centers for Excellence in Developmental Disabilities Education, Research and Service Training and Assistive Technology Program Technical Assistance and Data Collection Additional information included in Continuation Pages				

(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)*: CHRISTOPHER W. POULOS

31c. DATE SIGNED

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
2	Option Period 1 University Centers for Excellence in Developmental Disabilities Education, Research and Service Training and Assistive Technology Program Technical Assistance and Data Collection Additional information included in Continuation Pages (Option Line Item) Period of Performance: 09/30/2027 to 09/29/2028				
3	Option Period 2 University Centers for Excellence in Developmental Disabilities Education, Research and Service Training and Assistive Technology Program Technical Assistance and Data Collection Additional information included in Continuation Pages (Option Line Item) Period of Performance: 09/30/2028 to 09/29/2029				
4	Option Period 3 University Centers for Excellence in Developmental Disabilities Education, Research and Service Training and Assistive Technology Program Technical Assistance and Data Collection Additional information included in Continuation Pages (Option Line Item) Continued ...				

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. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE

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

38. S/R ACCOUNT NUMBER	39. S/R VOUCHER NUMBER	40. PAID BY

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 REC'D *(YY/MM/DD)*	42d. TOTAL CONTAINERS

NAME OF OFFEROR OR CONTRACTOR

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Period of Performance: 09/30/2029 to 09/29/2030				
5	Option Period 4 University Centers for Excellence in Developmental Disabilities Education, Research and Service Training and Assistive Technology Program Technical Assistance and Data Collection Additional information included in Continuation Pages (Option Line Item) Period of Performance: 09/30/2030 to 09/29/2031				

SECTION A - Solicitation/Contract Form

Contract to perform the work described in Section C, entitled, “Statement of Work.”

SECTION B - Supplies or Services and Prices/Costs

B.1 BRIEF DESCRIPTION OF SERVICES

University Centers for Excellence in Developmental Disabilities Education, Research and Service Training and Assistive Technology Program Technical Assistance and Data Collection

B.2 TYPE OF CONTRACT

The contract type awarded is a Cost Plus Fixed Fee.

B.3 SEVERABLE SERVICES

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

B.5 CONSIDERATION AND PAYMENT (CPFF – Severable Services)

In consideration of satisfactory performance of the work described in Section C, the contractor shall be reimbursed the cost plus fixed fee amount stated below for the base period and option periods (if exercised).

In consideration of satisfactory performance of the work described in Section C, the contractor shall be reimbursed up to the estimated cost plus fixed fee amount stated below for each of the CLINs (if exercised). If the options are exercised funding will be obligated by modification to the contract.

Period	Cost	Fee	Grand Total
Base Period			
Option Period 1			
Option Period 2			
Option Period 3			
Option Period 4			

TOTAL Potential Value inclusive of all CLINS: $_____

SECTION C - Description/Specifications/Statement of Work

University Centers for Excellence in Developmental Disabilities Education, Research and Service Training and Assistive Technology Program Technical Assistance and Data Collection

C.1 PROGRAM DESCRIPTION AND BACKGROUND

Purpose

The purpose of this project is for the Administration for Community Living (ACL), Administration on Disabilities (AoD), Office of Intellectual and Developmental Disabilities (OIDD) and Office of Interagency Innovation to contract for a performance-based arrangement for providing:

1. Coordinated, comprehensive, and specialized T/TA to the 67 University Centers for Excellence in Developmental Disabilities Education, Research and Service (UCEDDs); and

2. Coordinated, comprehensive, and specialized T/TA to the 56 Assistive Technology Programs (AT Programs), including operation of data collection, reporting, and dissemination systems.

Background

Developmental Disabilities Assistance and Bill of Rights Act

The Administration on Disabilities (AoD) is the Federal agency responsible for implementation and administration of the Developmental Disabilities Assistance and Bill of Rights Act of 2000 (DD Act of 2000) (42 U.S.C. 15001, et seq.). Consistent with Administration on Disabilities (AoD) usage, references in this document to people with developmental disabilities may also be expressed as people with intellectual and developmental disabilities (I/DD).This agency is located within the Administration for Community Living (ACL), a component of the U.S. Department of Health and Human Services (HHS).
The DD Act of 2000 authorizes support and assistance to States, public agencies, and private, non-profit organizations, including faith-based and community organizations, to assure that individuals with developmental disabilities and their families participate in the design of and have access to services, supports, and other assistance and opportunities that promote independence, productivity, integration, and inclusion into the community.
As defined in the DD Act of 2000, the term "developmental disabilities" means a severe, chronic disability of an individual that is attributable to a mental or physical impairment or combination of mental and physical impairments that are manifested before the individual attains age 22 and are likely to continue indefinitely. Developmental disabilities result in substantial limitations in three or more of the following functional areas: self-care, receptive and expressive language, learning, mobility, self-direction, capacity for independent living, and capacity for economic self-sufficiency.
There are four programs funded under the DD Act of 2000:

1. State Councils on Developmental Disabilities;
2. State Protection and Advocacy Systems;

3. National Network of University Centers for Excellence in Developmental Disabilities, Education, Research, and Service; and
4. Projects of National Significance.

The DD Act of 2000 identifies a number of significant findings, including:

- Disability is a natural part of the human experience that does not diminish the right of individuals with developmental disabilities to enjoy the opportunity for independence, productivity, integration, and inclusion into the community.
- Individuals whose disabilities occur during their developmental period frequently have severe disabilities that are likely to continue indefinitely.
- Individuals with developmental disabilities often require lifelong specialized services and assistance, provided in a coordinated manner by many agencies, professionals, advocates, community representatives, and others to eliminate barriers and to meet the needs of such individuals and their families.

In accordance with policies set out in the DD Act of 2000, AoD seeks to support and to ensure that:

> (1) individuals with developmental disabilities, including those with the most severe developmental disabilities, are capable of self-determination, independence, productivity, and integration and inclusion in all facets of community living, through the provision of community services, individualized supports, and other forms of assistance;
>
> (2) individuals with developmental disabilities and their families have competencies, capabilities, and personal goals that are recognized, supported, and encouraged, and any assistance to such individuals should be provided in an individualized manner, consistent with the unique strengths, resources, priorities, concerns, abilities, and capabilities of such individuals;
>
> (3) individuals with developmental disabilities and their families are the primary decision makers regarding the services and supports such individuals and their families receive, including regarding choosing where the individuals live from available options, and play decision-making roles in policies and programs that affect the lives of such individuals and their families;
>
> (4) services, supports, and other assistance are provided in a manner that demonstrates respect for individual dignity, personal preferences, and cultural differences;
>
> (5) specific efforts are made to ensure that individuals with developmental disabilities from racial and ethnic minority backgrounds and their families enjoy increased and meaningful opportunities to access and use community services, individualized supports, and other forms of assistance available to other individuals with developmental disabilities and their families;
>
> (6) recruitment efforts in disciplines related to developmental disabilities relating to pre-service training, community training, practice, administration, and policymaking focus on bringing larger numbers of racial and ethnic minorities into the disciplines in order to provide appropriate skills, knowledge, role models, and sufficient personnel to address the growing needs of an increasingly diverse population;

(7) with education and support, communities are accessible to and responsive to the needs of individuals with developmental disabilities and their families and are enriched by full and active participation in community activities, and contributions, by individuals with developmental disabilities and their families;

(8) individuals with developmental disabilities have access to opportunities and the necessary support to be included in community living, have interdependent relationships, live in homes and communities, and make contributions to their families, communities, and States, and the Nation;

(9) efforts undertaken to maintain or expand community-based living options for individuals with disabilities are monitored in order to determine and report to appropriate individuals and entities the extent of access by individuals with developmental disabilities to those options and the extent of compliance by entities providing those options with quality assurance standards;

(10) families of children with developmental disabilities have access to and use of safe and appropriate childcare and before-school and after-school programs, in the most integrated settings, in order to enrich the participation of the children in community living;

(11) individuals with developmental disabilities have access to and use of public transportation, in order to be independent and directly contribute to and participate in all facets of community living; and

(12) individuals with developmental disabilities have access to and use of recreational, leisure, and social opportunities in the most integrated settings, in order to enrich their participation in community living.

ACL's vision is that all people, regardless of age and disability, live with dignity, make their own choices, and participate fully in society. AoD shares in ACL's mission to maximize the independence, well-being, and health of people with developmental disabilities, their families and other members of their support system.

The AoD's OIDD requires a performance-based arrangement for providing responsive, comprehensive, and specialized training and technical assistance (T/TA) to University Centers for Excellence in Developmental Disabilities Education, Research and Service (UCEDD), defined as follows:

- *Responsive* means addressing UCEDD's needs as it relates to implementing grants from multiple funding sources and being adaptive to multiple stakeholders (e.g., federal funders, host universities, community partners).
- *Comprehensive* means a broad array of T/TA that starts with a foundation of resources which can be broadly applied yet is responsive to the needs of UCEDDs of varying sizes (small, medium, large) and includes T/TA which addresses highly complex, individualized issues and needs.
- *Specialized* means T/TA that is tailored to the unique role of UCEDDs as the only federally legislated and funded network of Centers providing basic and applied research, model and demonstration services, and interdisciplinary training for professionals and community members who work with people with I/DD and their families. T/TA must be highly customized to meet the needs of this network – both as a collective network and on an individual basis.

Coordinated T/TA

OIDD administers the UCEDD program under the Developmental Disabilities Assistance and Bill

of Rights of 2000 (DD Act) (42 U.S.C. 15001 et seq.). UCEDDs are funded to provide leadership in, advise Federal, State, and community policymakers about, and promote opportunities for individuals with developmental disabilities to exercise self-determination, be independent, be productive, and be integrated and included in all facets of community life (Section 153 (a)(1)). UCEDDs are defined as interdisciplinary education, research, and public service units of universities or public or non-profit entities associated with universities that engage in four core functions, addressing directly or indirectly, one or more of the areas of emphasis established under the DD Act:

- Interdisciplinary pre-service preparation and continuing education of students and fellows, which may include the preparation and continuing education of leadership, direct service, clinical, or other personnel to strengthen and increase the capacity of States and communities.
- Community services that provide training or T/TA for individuals with developmental disabilities, their families, professionals, paraprofessionals, policymakers, students, and other members of the community; and that may provide services, supports, and assistance for the persons described demonstration and model activities.
- Research, which may include basic or applied research, evaluation, and the analysis of public policy in areas that affect or could affect, either positively or negatively, individuals with developmental disabilities and their families.
- Dissemination of information related to activities undertaken related to developmental disabilities, especially, dissemination of information that demonstrates that the network of expertise that may be accessed and applied in diverse settings and circumstances.

UCEDDs are required by the DD Act to leverage funds to carry out these core functions; thereby creating a need for coordinated T/TA to UCEDDs. This effort is to ensure that T/TA is provided to support UCEDDs as they manage and implement grants from multiple federal and other agencies as a requirement to be a UCEDD.

Comprehensive T/TA

To be effective interdisciplinary training, community service, research, and research to practice organizations, UCEDDs must be adept at managing multiple programs and initiatives while simultaneously focusing on the mission of the work, thereby requiring comprehensive T/TA that addresses a wide array of issues across higher education, disability, and organizational contexts. UCEDDs require a foundation to advance knowledge in two main areas:

(1) UCEDD core functions and disability content, and
(2) UCEDD organizational competency.

Given the comprehensive nature of T/TA, these two areas necessarily overlap and require a foundational program to advance work in the following areas:

- The UCEDD program, including the history of the program and the disability movement.
- Emerging issues in I/DD and related areas of emphasis.
- Various effective approaches to training and advocacy focused on the productivity, integration and inclusion of individuals with developmental disabilities in all aspects of community life.
- Standard UCEDD practices for individual and systemic change, interdisciplinary training, community services, research and dissemination of information.

- Outcome and impact measurement and evaluation of UCEDD effectiveness.
- Planning, implementation, and continuous improvement of UCEDD activities.
- Maintaining and strengthening a Consumer Advisory Committee (CAC) to ensure meaningful participation of individuals with developmental disabilities, family members, and other community representatives in UCEDD planning, implementation, evaluation, and priority-setting.
- Personnel management.
- Financial/Fiscal management.
- Emerging issues in the disability field and how they relate to emerging and promising practices in effective UCEDD operations.
- Strategies for scaling, replication, and sustainability of effective practices and initiatives to expand impact across communities and systems.
- Collaboration with other entities funded under the DD Act such as the:
    - State Councils on Developmental Disabilities
    - State Protection and Advocacy Systems
- Collaboration with key partners i.e. federal, state, and local DD agencies, state self-advocacy groups, other relevant Federally funded and non-federally funded entities and programs, including those funded under IDEA and WIOA to ensure UCEDDs have a contributing role in improving outcomes for people with I/DD.

Specialized T/TA

UCEDDs comprise a unique, highly specialized national network of interdisciplinary Centers federally legislated and funded to conduct basic and applied research, model and demonstration services, interdisciplinary training for professionals and community members who work with people with I/DD and their families, and information dissemination, including dissemination of information that demonstrates that the network is a national and international resource. There is no other comparable network in the U.S. and its territories, therefore, it requires specialized T/TA tailored to the unique needs and role of the UCEDD network.

T/TA must be highly customized to meet the needs of this network – both as a collective network and on an individual basis. The UCEDDs have the same purpose and core functions, but face different circumstances in each state and territory, requiring T/TA be both broad based and individualized when needed. In particular, there is a need for T/TA that addresses the resource needs of the UCEDDs by staying current on disability trends, conducting analyses of emerging issues, and supporting the overall organizational stability of each individual UCEDD by strengthening the role and performance of the UCEDD Network as a whole through specialized T/TA. Together, these activities improve quality of life for people with I/DD, and enhance the systems serving people with I/DD, resulting in full participation in all aspects of community life.

<u>Program Goals and Outcomes</u>

OIDD requires a performance-based contract for providing coordinated, comprehensive, and specialized T/TA to the 67 UCEDDs. Under a performance-based contract, performance will be measured by the outcomes achieved. This statement of objectives outlines the desired results and expected outcomes to be achieved for the work performed. Appendix A includes a logic model, which is a graphic description of UCEDD T/TA inputs, activities, outputs, and outcomes. These services should be reliable, effective, efficient, and responsive to the field and work towards

achieving the long term outcomes of:

- Positioning UCEDDs and the UCEDD Network as leaders in advancing systems change, capacity building, and advocacy at the local, state/territory, and national, levels, and as national resources with specialized expertise that can be applied in multiple settings and circumstances.

- Increasing the capacity of UCEDDs to provide leadership in, advise Federal, State, and community policymakers about, and promote opportunities that lead to individuals with I/DD exercising self-determination, becoming independent, productive, integrated, and included in all facets of community life; and

- Increasing UCEDD's quality of data collection for Program Performance reporting (PPR) demonstrating the UCEDD Network's collective impact on the local, state, national, international levels.

Under the direction of the COR, the Contractor is responsible for the provision of comprehensive, coordinated, specialized T/TA to UCEDDs and shall plan, arrange, and provide all the required personnel, consultants, resource facilities, and equipment needed to fulfill the requirements of the contract in the most cost-efficient manner by:

- Designing T/TA that provides for a foundation of fundamental skills and knowledge to reserve resources to address more individualized, specialized T/TA for highly complex needs;
- Enhancing the use of technology for providing T/TA in the most cost-efficient manner; and
- Bolstering the use of peer-to-peer techniques to maximize knowledge transfer across the Network.

The short-term outcomes for the contract are that, by the end of each project year, at least 80 percent of participating UCEDD leadership, new directors, and staff will demonstrate measurable increases in knowledge, skills, and confidence in the following areas, as evidenced by, training evaluations, self-assessments, completion data, or follow-up feedback.

1. UCEDD Foundations and Emerging Disability Issues

At least 80 percent of participants will demonstrate increased knowledge of:

- the UCEDD program, including its history, purpose, and relationship to the disability rights movement;
- historical, current, and emerging issues in the I/DD and broader disability fields, including pressing issues such as restraint, supported decision-making, and employment; and
- the implications of these issues for interdisciplinary training, community services, research, information dissemination, and engagement with unserved and underserved communities.

2. Leadership, Compliance, and Effective UCEDD Operations

At least 80 percent of participants, including new directors, will demonstrate increased knowledge of:

- key UCEDD leadership roles and responsibilities, including the DD Act, CAC requirements, leveraging funds, and other core leadership functions;

- financial and fiscal management practices necessary to maintain compliance with federal requirements; and
- proven and standardized practices that strengthen UCEDD operations and improve the Network's ability to carry out its mission.

3. Strategy, Advocacy, Collaboration, and Dissemination
At least 80 percent of participants will demonstrate increased knowledge of:

- effective strategies for addressing emerging issues and the evolving needs of individuals with I/DD and their families;
- effective approaches to training, advocacy, and systems change that promote productivity, integration, and full inclusion in community life;
- strategies for collaboration, peer-to-peer learning, and knowledge exchange with other UCEDDs and subject matter experts; and
- Effective dissemination and outreach strategies to increase awareness, accessibility, and utilization of UCEDD services among individuals with I/DD and their families, including the use of plain language, digital platforms, and community-based outreach.

4. Evaluation, Performance Improvement, and Evidence-Based Practice
At least 80 percent of participants will demonstrate increased knowledge of:

- effective techniques for measuring and evaluating UCEDD effectiveness, including evaluation of the four core functions; and
- evidence-based and promising practices, including use of T/TA web-library resources, to strengthen implementation, performance, and continuous quality improvement.

By the end of each project year, and relative to an established baseline, the project will achieve the following intermediate outcomes:

1. Strengthened UCEDD Leadership, Operations, and Statutory Compliance

- At least 75 percent of UCEDDs receiving targeted T/TA will demonstrate improved organizational performance, operations, and outputs, including stronger leadership capacity, improved implementation of UCEDD roles and responsibilities, and improved achievement and maintenance of statutory and fiscal compliance.
- At least 80 percent of UCEDD New Directors participating in onboarding and leadership supports will report increased confidence and demonstrate improved capacity to lead the UCEDD.
- At least 75 percent of UCEDDs receiving operational T/TA will implement at least one improvement in organizational infrastructure, internal processes, leveraging of funds, or other core operational practices.
- At least 90 percent of identified compliance issues addressed through T/TA will show documented progress toward resolution or full resolution within the project year.

2. Improved Strategic Planning, Evaluation, and Use of Performance Data

- At least 75 percent of UCEDDs receiving T/TA in planning, evaluation, or data use will demonstrate improved capacity to use strategic planning, evaluate five-year goals and objectives, and apply performance information to strengthen decision-making and continuous quality improvement.
- At least 75 percent of UCEDDs will demonstrate improved use of NIRS/PPR data beyond compliance reporting for planning, management, or program improvement.
- At least 75 percent of UCEDDs will show improvement in the quality, completeness, timeliness, or consistency of Program Performance Reporting data.
- Access to timely, actionable performance information through a real-time data dashboard or comparable data system will improve annually, enabling UCEDDs to identify trends, monitor progress, and respond more effectively to performance needs.
- NIRS data entry forms, reporting processes, and PPR structure and usability will be improved through contractor-supported recommendations, testing, tools, or guidance adopted with ACL/COR approval.

3. Increased Coordination, Peer Exchange, and Cross-System Engagement

- At least 75 percent of participating UCEDDs will demonstrate increased collaboration with DD Act entities, relevant peers, and cross-system partners to improve performance, problem-solving, and shared learning.
- Participation in regional, cross-state, and peer mentorship activities will increase annually from baseline.
- Participation in DD Network and cross-system engagement activities will increase annually from baseline.
- Utilization of site visits and peer-to-peer exchanges as mechanisms for improvement will increase annually from baseline.

4. Modern Dissemination, Outreach, and Stakeholder Engagement

- At least 75 percent of UCEDDs receiving dissemination and outreach T/TA will demonstrate improved dissemination and outreach strategies that implement strategic, accessible, and modern practices to expand awareness, engagement, and utilization of UCEDD initiatives and services.
- At least 75 percent of participating UCEDDs will demonstrate increased engagement with stakeholders, including DD Network partners, CACs, parent organizations, and other community partners.
- At least 75 percent of participating UCEDDs will demonstrate stronger capacity to communicate UCEDD impact through accessible products, success stories, and other dissemination tools.

5. Greater Use, Scalability, and Sustainability of Evidence-Informed Practices

- At least 75 percent of UCEDDs receiving content-focused or implementation T/TA will demonstrate increased ability to apply evidence-based, promising, or innovative practices in the implementation of the UCEDD core functions and in addressing key and emerging issues affecting people with I/DD and their families.

- Scalability and sustainability of effective practices will increase annually, with participating UCEDDs demonstrating greater capacity to design, replicate, adapt, and sustain evidence-informed and promising practices.
- At least 60 percent of participating UCEDDs will adopt, adapt, replicate, or sustain at least one evidence-informed or promising practice supported through the project.
- At least 75 percent of participating UCEDDs will report improved capacity to address key and emerging issues through training, T/TA, research, service, or dissemination activities.

6. Increased Participation of People with I/DD in UCEDD Work

- At least 75 percent of participating UCEDDs will demonstrate increased inclusion of people with disabilities, including people with I/DD from communities, in research, training, service, dissemination, governance, and other UCEDD core functions.
- Participation of people with I/DD in UCEDD activities will increase annually from baseline.
- At least 75 percent of participating UCEDDs will demonstrate improved strategies for meaningful engagement at multiple levels of UCEDD work.

7. Increased Demonstration of UCEDD Leadership and Network Impact

- At least 75 percent of participating UCEDDs will demonstrate increased ability to show leadership at the community, state/territory, regional, and national levels and to document the UCEDD Network's collective impact through stronger reporting, success examples, and performance information.

Assistive Technology Act of 1998, as Amended

The 21st Century Assistive Technology Act (AT Act of 1998, as Amended, P.L. 105-394, codified at 29 U.S.C. § 3001 et seq.) under Section 4 authorizes formula grants to support State and Territory Assistive Technology Programs (AT Programs) administered by the Administration for Community Living (ACL). The AT Act's purpose is to increase knowledge about, access to, and acquisition of assistive technology (AT) devices and services for individuals with disabilities and older Americans.

As defined in the AT Act, "assistive technology device" means any item, piece of equipment, or product system, whether acquired commercially, modified, or customized, that is used to increase, maintain, or improve functional capabilities of individuals with disabilities. "Assistive technology service" means any service that directly assists an individual with a disability in the selection, acquisition, or use of an assistive technology device.

Section 4 of the AT Act provides 56 formula grants to support an AT Program in each of the 50 states, as well as the District of Columbia, Puerto Rico, American Samoa, Guam, the Northern Mariana Islands, and the U.S. Virgin Islands.

1.7 AT Program Requirements and Activities

AT Programs focus on improving the provision of AT through comprehensive, statewide programs that are consumer responsive. The goal of these programs is to increase access to and acquisition of AT through an integrated set of state-level activities and state leadership activities.

The 2004 and 2022 reauthorizations of the AT Act required a common set of activities to be provided by all AT Programs (with some limited exceptions) to create consistency among grantees. Required activities include:

State-Level Activities:

- State Financing Activities - Alternative financing programs, financial-loan programs, interest buy-down programs, revolving loan funds, loan guarantee or insurance programs, or other methods of financing the purchase of AT devices and services
- Device Reutilization Programs - Programs that provide for the exchange, repair, recycling, or other reutilization of AT devices
- Device Loan Programs - Short-term loans of AT devices to individuals, employers, public agencies, or others
- Device Demonstrations - Opportunities for individuals with disabilities and their family members, guardians, advocates, authorized representatives, employers, and other interested parties to learn about and experience AT devices

State Leadership Activities:

- Training and Technical Assistance - For individuals with disabilities, family members, service providers, educators, employers, and others
- Public Awareness - Activities to provide information to targeted individuals and entities in the state about the availability and benefits of AT
- Information and Assistance Services - Assistance in accessing AT devices and services
- Coordination and Collaboration - Activities to enhance coordination among state programs and improve access to AT

AT Programs are required to serve people with all types of disabilities, of all ages, in all environments. Programs must also serve family members, service providers, educators, therapists, employers, health and rehabilitation professionals, AT vendors, procurement officials, and other interested parties.

Data Reporting Requirements

Section 4 of the AT Act requires specific data reporting on services provided via the required state-level and leadership activities. AT Programs submit annual progress reports (AT APRs) and three-year state plans for assistive technology (State Plans for AT) through approved information collection instruments authorized by the Office of Management and Budget (OMB).

The Office of Interagency Innovation within ACL requires coordinated, comprehensive, and

specialized T/TA to the 56 AT Programs to ensure:

- Consistent implementation of AT Act requirements across all states and territories
- High-quality data collection for federal reporting and program evaluation
- Evidence-based practices in AT service delivery
- Coordination with other disability programs and stakeholders
- Public access to AT Program data and resources

C.2 STATEMENT OF WORK - Severable Services

The Contractor shall furnish all of the necessary personnel, materials, services, facilities, (except as otherwise specified herein), and otherwise do all the things necessary for or incident to the performance of the work as set forth below:

UCEDD TRAINING AND TECHNICAL ASSSISTANCE (T/TA) TASKS / ACTIVITIES
The T/TA activities are organized around four main areas:

(1) Project Management and Evaluation
(2) Strengthening Capacity, Practice, and Performance
(3) Coordination
(4) Information Management

The following statement of objectives is based on this organizing framework for T/TA.

Project Management and Evaluation

Before operating any system or workflow that collects, stores, transmits, or processes PII on behalf of ACL, the Contractor shall support ACL in completing required privacy compliance activities, including data inventory, privacy threshold analysis, Privacy Impact Assessment support, records analysis, and review of whether a SORN or other notice is required. The Contractor shall collect only the minimum information necessary for authorized purposes.

a. Strategic Planning, Logic Model, and Performance Measurement and Evaluation Matrix

The Contractor shall develop, maintain, and annually update a 5-year strategic plan, logic model, and performance measurement and evaluation matrix for the delivery of T/TA under this contract. The strategic plan and logic model shall clearly identify the goals, objectives, tasks, activities, outputs, and intended outcomes that will guide contract implementation and support achievement of project impacts to the maximum extent possible. The performance measurement and evaluation matrix shall align with the strategic plan and logic model and identify, at a minimum, the corresponding performance measures, indicators, data sources, methods of assessment, targets, timelines, and reporting frequency used to monitor implementation, evaluate progress, and assess achievement of contract outcomes. The strategic plan, logic model, and performance measurement and evaluation matrix shall be guided by the following principles:

i. *High-Quality, Efficient, and Outcome-Driven:* Deliver comprehensive, coordinated, and specialized T/TA that is responsive to the needs of the UCEDD network while maximizing reach, effectiveness, and cost-efficiency.

ii. *Evidence-Based:* Use evidence and evidence-based strategies, resources, and tools, to the extent available, to design, deliver, and refine T/TA.

iii. *Continuous Improvement:* Apply practical and effective methods, tools, and approaches that strengthen service quality, efficiency, cost-effectiveness, and outcomes.

iv. *Tiered T/TA Delivery:* Use a hierarchical approach to T/TA delivery that maximizes broadly applicable resources and group-based strategies, while reserving more intensive and individualized support for complex or high-priority needs.

The Contractor shall incorporate applicable ACL and HHS priorities, such as the Make America Healthy Again (MAHA) initiative and ACL operational priorities, as directed by the COR, and shall update the strategic plan, logic model, and performance measurement and evaluation matrix, as needed, to reflect any changes in federal priorities during the period of performance.

b. Project Advisory Committee

The Contractor shall establish and maintain a multi-stakeholder, representative Project Advisory Committee to provide guidance on the design, implementation, and continuous improvement of the T/TA delivered under this contract. The committee shall include, as appropriate, UCEDD representatives, subject matter experts, individuals with disabilities, family members, and other key stakeholders, and shall meet at least two times per year.

i. The committee shall advise the Contractor on T/TA priorities, emerging needs, accessibility, dissemination strategies, and resource development. At a minimum, this guidance shall inform training, webinars, tools, and technical assistance approaches that support grantees in:
    1. Obtaining and budgeting for accessible communication and language access services;
    2. Addressing systemic issues through communities of practice, expert consultation, visiting professor models, and regular problem-solving sessions; and
    3. Identifying and disseminating vetted resources and vendor information related to accessible communication and dissemination, including ASL, closed captioning, screen reader accessibility, oral interpretation, plain language, accessible web platforms, podcasts, online training modules, and publication supports.

c. Ongoing Performance Monitoring and Reporting

The Contractor shall establish and implement a project management and performance monitoring process to regularly identify emerging T/TA needs, monitor service delivery, assess progress toward outcomes, and support timely course correction. At a minimum, the Contractor shall submit monthly reports to the COR that summarize:

i. Emerging and recurring T/TA needs, trends, and issues across the UCEDD network;

ii. T/TA provided during the reporting period, including scope, modality, topic, and level of effort;

iii. Progress toward project goals, objectives, outputs, and outcomes;

iv. Key risks, barriers, and mitigation strategies; and

v. Recommended adjustments to the strategic plan, logic model, goals, objectives, tasks, and activities, as needed and subject to federal review and approval.

d. T/TA Services Performance Dashboard

All Federal information, including backups, exports, logs containing sensitive data, and data stored on portable or removable media, shall be encrypted at rest and in transit in accordance with HHS policy and approved cryptographic standards. Unencrypted storage of PII on portable/removable media is prohibited unless expressly authorized in writing by ACL.

The Contractor shall design, develop, implement, maintain, and continuously update a secure, real-time, Section 508-compliant, interactive T/TA Services Performance Dashboard, subject to COR approval. The dashboard shall support performance reporting, transparency, identification of risks and issues, and continuous quality improvement across the UCEDD network. At a minimum, the dashboard shall:

i. Track and report T/TA services delivered under this contract to provide visibility into UCEDD program performance and needs, support transparency, identify program risks and issues, inform continuous quality improvement across the UCEDD network, and support the development and refinement of T/TA mitigation strategies for UCEDD programs identify to be at risk;

ii. Allow ACL/OIDD to review information at multiple levels, including national or network-wide, state, UCEDD, institutional, and project levels, as appropriate;

iii. Provide accessible, user-friendly visualizations for multiple audiences, including ACL/OIDD leadership, UCEDD directors, policymakers, partners, and the public, as appropriate;

iv. Display key service delivery metrics, including service volume, topic distribution, timeliness, intensity, modality, and level of engagement;

v. Track the development, maintenance, dissemination, inventory, and use of T/TA tools, resources, and infrastructure, including the annual review and updating of materials and the archiving of outdated content;

vi. Provide end-to-end visibility into customized and responsive T/TA, including request intake, review, approval, scope, delivery, follow-up, and closure;

vii. Display indicators related to response time, completion timeliness, service intensity, delivery mode, high-demand topics, recurring barriers, and emerging issues; and

Support regular sharing of dashboard findings, trends, and performance insights with UCEDD leadership through webinars, written summaries, and network meetings.

e. Evaluation and Continuous Quality Improvement

Throughout the period of performance, the Contractor shall improve service performance, reliability, quality, and cost-effectiveness through ongoing formative assessment and annual summative evaluation, using the performance measurement and evaluation matrix developed under subsection (a) to guide monitoring, analysis, and reporting.

i. *Formative Assessment:* The Contractor shall implement an ongoing self-monitoring process, informed by the performance measurement and evaluation matrix, to assess progress on project activities, service quality, efficiency, and progress toward contract outcomes, and shall report findings to the COR on a monthly basis.

ii. *Summative Evaluation:* The Contractor shall conduct and submit an annual summative assessment to OIDD, using the performance measurement and evaluation matrix to assess the extent to which the T/TA delivered under this contract has improved UCEDD capacity and performance in ways that contribute to meaningful outcomes for individuals with I/DD and their families. The summative assessment shall address the extent to which the T/TA has helped UCEDDs to:

1. Strengthen their capacity to serve as leaders in systems change, capacity building, and advocacy at the national, state or territory, and local levels in ways that improve access, participation, inclusion, and system responsiveness for individuals with I/DD and their families;
2. Strengthen the UCEDD Network's role as a national resource with substantive expertise that can be applied across settings and circumstances to improve policies, programs, services, supports, and community outcomes for individuals with I/DD and their families;
3. Increase their capacity to lead, advise federal, state, and community policymakers, and promote opportunities for individuals with I/DD to exercise self-determination and live independently, productively, and fully included in community life;
4. Improve the quality and usefulness of Program Performance Reporting data to better demonstrate the collective impact of the UCEDD Network on individuals with I/DD and their families at the local, state, national, and international levels; and
5. Assess the satisfaction of UCEDD personnel who received individualized or customized T/TA, including the perceived relevance, timeliness, quality, and usefulness of the assistance provided, and use the results to inform service improvements and future T/TA delivery.

Strengthening Capacity, Practice, and Performance

The Contractor shall achieve project goals by implementing a sequenced, tiered T/TA approach that ranges from broad-based information sharing and foundational skill building to targeted, intensive, and highly customized assistance. The approach shall strengthen the knowledge, skills, practices, and performance of UCEDD leadership, faculty, staff, and CAC members and shall

respond to varying levels of readiness, capacity, and complexity across the UCEDD Network.

The Contractor shall provide universal, targeted, and individualized T/TA to strengthen UCEDD leadership, infrastructure, operations, dissemination, impact measurement, and overall program performance, including by:

a. Developing, maintaining, and updating a modern, dynamic T/TA website that:

   i. Serves as the central, continuously updated hub for UCEDD resources, tools, peer examples, impact materials, and T/TA opportunities;
   ii. Is user-friendly, searchable, fully accessible, and Section 508 compliant;
   iii. Maintains a curated, searchable, and continuously updated library of tiered resources and materials, ranging from foundational to advanced, developed in-house or by proven experts, that support UCEDDs in implementing federally mandated authorities and addressing current, emerging, and priority issues in disability and related policy and practice areas, including but not limited to:
      1. UCEDD core functions, including interdisciplinary preservice training, community service, research, and information dissemination;
      2. Disability topics of national and cross-cutting significance, such as housing, employment, self-advocacy, education, early intervention, childcare, and other priority issue areas;
      3. Current and relevant impact examples, practice examples, and documented results from grantees, with an annual summary of examples collected throughout the year;
      4. Infrastructure and operations, including leveraging funds, fiscal management, CAC training and engagement, financial stability and sustainability, planning and evaluation, federal reporting, monitoring, personnel management, and leadership development;
      5. Emerging, evidence-informed, and promising practices within the UCEDD Network that may be adapted or replicated by other UCEDDs; and
      6. Practical examples, implementation tools, and case studies from UCEDDs;

   iv. Includes a content structure, navigation design, and resource organization approved by the COR; and
   v. Uses website analytics, user feedback, and T/TA demand trends to guide ongoing refinement, content development, and resource prioritization.

b. Developing and delivering high-quality training and peer-learning opportunities that include:

   i. A comprehensive orientation for UCEDD Directors covering leadership, DD Act requirements, CAC support, and core administrative and programmatic responsibilities;
   ii. Leadership development curricula and skill-building opportunities for UCEDD staff and emerging leaders;
   iii. Disability-specific and topic-specific training responsive to current and emerging issues;
   iv. Training to strengthen UCEDD infrastructure, operations, compliance, planning, and performance;

v. Regional, cross-network, and topic-based peer-learning forums that support problem solving and exchange of effective practices; and

vi. Training on the use of NIRS/PPR and related performance data to support strategic communications, visibility, impact messaging, and decision-making beyond compliance reporting.

c. Providing timely, accurate, and practical expert analysis, decision-support resources, peer examples, and responsive consultation to assist UCEDDs and OIDD in addressing emerging policy, programmatic, operational, and disability-related issues.
d. Providing individualized, outcome-oriented T/TA and peer connection strategies to help UCEDDs address complex challenges by maintaining a cadre of proven experts and web-based mechanisms that:

i. Provide timely, accurate, and practical resources, supports, and T/TA to UCEDD leadership, faculty, staff, and CAC members;

ii. Strengthen capacity, leadership, and problem-solving within individual UCEDDs and across the Network;

iii. Support strategic peer-to-peer networking, including identification of proven experts and linkages among UCEDDs through the T/TA website and related mechanisms;

iv. Facilitate formal peer mentorship for UCEDD Directors, including support for new Directors and those facing complex leadership or operational challenges; and

v. Support site visits, peer consultation, and other structured learning opportunities to observe scalable programs, effective practices, and successful operational approaches.

e. Strengthening UCEDD dissemination capacity and public awareness of UCEDD roles, contributions, and impact on people with I/DD and their families by:

i. Providing T/TA to strengthen and modernize UCEDD dissemination and strategic communications capacity, including plain language, accessible dissemination, digital engagement, media relations, audience-centered message development, and evidence-informed impact communication approaches, with targeted support for UCEDDs needing additional assistance to improve dissemination effectiveness;

ii. Supporting UCEDDs in translating research, training, service, and systems-change outcomes into accessible, audience-specific dissemination products, such as policy briefs, impact summaries, infographics, videos, and executive summaries, for people with I/DD and their families, self-advocates, policymakers, funders, partners, and other key stakeholders;

iii. Developing and promoting data-informed tools, messaging, and outreach strategies that help UCEDDs communicate impact beyond compliance reporting, modernize

dissemination practices, and expand public awareness of UCEDD contributions, including by:

1. Developing tools and templates to support the use of NIRS/PPR and other performance data to communicate outcomes, demonstrate return on investment, and show how UCEDD activities improve opportunities, services, systems, and quality of life for people with I/DD and their families;
2. Promoting consistent national messaging that elevates awareness of the UCEDD Network's collective contributions while preserving individual UCEDD identity and state-specific impact;
3. Identifying and amplifying exemplary UCEDD dissemination, outreach, and public awareness approaches as replicable practices across the Network;
4. Supporting UCEDDs in documenting and communicating the impact of their work on people with I/DD and their families, including outcomes related to independence, community inclusion, informed choice, stability in community living, access to services and supports, and improved quality of life; and
5. Advancing innovative, accessible, and data-informed outreach strategies, including digital engagement platforms, targeted communications campaigns, and partnerships with self-advocacy organizations, family organizations, faith-based organization and community-based entities.

f. Strengthening grantee program improvement, accountability, and strategic decision-making through an integrated impact measurement and data strategy by:

i. Operationalizing an approach, such as Trace the Line, that systematically connects:
   1. Federal investment;
   2. UCEDD activities and partnerships;
   3. Measurable outputs;
   4. Individual- and systems-level outcomes; and
   5. Demonstrated impact on people with developmental disabilities and their families.

ii. Conducting a comprehensive UCEDD Impact Portfolio of the 67 UCEDDs that conveys the Network's impact on people with developmental disabilities and their families by organizing, analyzing, and presenting findings in accessible, actionable formats. The Impact Portfolio shall:
   1. Systematically document and categorize UCEDD projects, activities, initiatives, and focus areas across the Network, linking each entry to intended beneficiaries, outcomes, and demonstrated impact for people with developmental disabilities and their families;
   2. Identify and highlight UCEDD work aligned with HHS strategic priorities, ACL strategic goals, and federal disability policy initiatives, including the outcome pathways through which such work advances inclusion, self-determination, community living, and family supports;
   3. Quantify and summarize impact using standardized fields, to the extent feasible, such as reach, outcomes achieved, populations served, settings, partner sectors, and evidence type, and translate these findings into clear, plain-language impact statements and summaries;
   4. Provide targeted T/TA to UCEDDs that are not effectively producing impact statements in order to strengthen their capacity to develop clear, data-informed,

audience-appropriate statements that communicate meaningful outcomes for people with developmental disabilities and their families;

5. Identify promising practices, innovative approaches, and replicable models, including the conditions needed for success, such as context, partnerships, staffing, resources, and implementation considerations;
6. Highlight the return on federal investment, including cost avoidance where feasible, leveraging of additional funds, and long-term infrastructure strengthening and capacity building;
7. Present findings in accessible formats, including interactive databases, visualizations, reports, and summary documents for ACL, UCEDDs, policymakers, partners, people with developmental disabilities and their families, and the public, as appropriate; and
8. Update the Impact Portfolio annually to reflect new initiatives, completed projects, shifts in priorities, and evolving HHS and ACL goals, and disseminate findings through the T/TA website and UCEDD meetings.

Coordination

a. Coordination with UCEDDs
The Contractor shall establish and maintain partner-focused, responsive working relationships with UCEDDs to strengthen coordination across the network and improve UCEDD operations, performance, outcomes, scalability of effective practices, and collective impact. At a minimum, the Contractor shall:

i. Provide coordinated support in the two primary areas of UCEDD need:
    1. UCEDD core functions and disability content; and
    2. UCEDD organizational competency, including leadership, management, systems, and infrastructure.

ii. Maintain regular communication and engagement with UCEDDs to identify needs, support timely problem-solving, inform responsive T/TA, and promote continuous quality improvement.

iii. Coordinate activities that strengthen UCEDD capacity to:
    1. Maintain or achieve statutory compliance;
    2. Improve program performance and operational effectiveness;
    3. Improve measurable outcomes and impact for individuals with I/DD and their families;
    4. Serve as leaders in systems change, capacity building, and advocacy at the local, state, territorial, and national levels; and
    5. Implement, adapt, and sustain effective, evidence-informed, and promising practices.

iv. Facilitate peer exchange, shared learning, and cross-center problem-solving among UCEDDs, including across regions, topic areas, and levels of organizational capacity, to accelerate adoption of effective practices and expand network-wide impact.

v. Coordinate support in a manner that reflects the multiple funding streams, institutional contexts, and stakeholder relationships within which UCEDDs operate.

vi. Strengthen UCEDD capacity to contribute to and demonstrate the collective impact of the UCEDD Network through coordinated learning, dissemination, and performance improvement.

vii. Support the identification, replication, adaptation, scaling, and broader utilization of effective practices, resources, tools, and innovations across the UCEDD Network.

b. Coordination with Other Key Stakeholders
The Contractor shall establish and maintain effective, partner-focused working relationships with key stakeholders to strengthen alignment, collaboration, and coordinated action across the broader disability and cross-system landscape. At a minimum, the Contractor shall:

i. Establish and maintain working relationships with the T/TA providers or contractors serving:
    1. State Councils on Developmental Disabilities;
    2. Protection and Advocacy Systems; and
    3. Independent Living programs and centers;
    4. for the purpose of strengthening collaboration AoD partners within and across states and territories.

ii. Identify, address, and help resolve barriers to effective DD Network coordination and joint action.

iii. Create and facilitate regional, national, and topic-based engagement opportunities that promote cross-state and cross-territory collaboration, peer exchange, and shared problem-solving.

iv. Advance cross-system engagement with key partners, including but not limited to vocational rehabilitation, education, healthcare, aging services, IDEA-funded systems, workforce systems under WIOA, and other relevant public and community-based systems.

v. Support coordinated responses to pressing and emerging disability issues affecting states and territories.

vi. Convene proven experts, representatives from the UCEDD Network, and federal and non-federal partners, as appropriate, to:
    1. Identify and examine emerging issues, needs, and promising practices;
    2. Address priority topics, including but not limited to interdisciplinary training, community responsiveness, and other evolving policy or practice issues; and
    3. Develop and disseminate guidance, tools, and other T/TA strategies that address emerging priorities and needs.

vii. Promote alignment of T/TA strategies, resources, and messaging across partner organizations, where appropriate, to reduce duplication, strengthen consistency, and increase collective impact.

Information Management

1. Provide for as long as it is needed a highly reliable and secure web-based information management system of services and supports that meets or exceeds customer requirements and expectations for electronic submission of the Annual OIDD/UCEDD program performance report (PPR)s.

2. Given the dynamics of the web-based information management market, establish an arrangement that easily accommodates change to any and all information management system maintained by the contractor.

3. Directly manage a flexible, transparent, and responsive federal reporting web-based information management system for as long as it is needed with interactive components that provides:

    a. A mechanism for UCEDDs to electronically store required documents submitted to the federal agencies (e.g. PPR), with embedded guidance for grantees to provide high quality activity descriptions.
    b. A mechanism for UCEDDs to electronically transfer to OIDD the required documents (e.g., PPR).
    c. In a timely manner, data files to federal staff (OIDD) based on federal agency specifications.

4. User testing, streamlined forms, enhanced guidance, reduced burden, comprehensive training

5. Streamline for better impact capture, format for marketing use, tools for UCEDDs to use their own data

6. Provide effective T/TA to UCEDD and federal staff on the web-based information management systems supported by this funding.

7. Prepare reports and provide data as requested in accordance with OIDD format and guidelines.

8. Directly manage a web-based information management system which can be accessed by the public that provides for full functionality to categorically search for past and current initiatives, activities and efforts undertaken by UCEDDs that meets OIDD's expectations.

9. Accessibility

    This contract is subject to Section 508 of the Rehabilitation Act (the Act) of 1973 (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998, and the Architectural and Transportation Barriers Compliance Board (Access Board) Electronic and Information Accessibility Provisions (36 CFR Part 1194). Section 508 of the Act requires that, unless an exception applies, all communications products and services that require a contractor or consultant to produce content in any format that is specifically

intended for publication on, or delivery via, a federally owned or federally funded website or intranet permit the following:

(1) Federal employees with disabilities to have access to and use information and data that is comparable to the access and use of information and data by federal employees who are not individuals with disabilities.

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

(Note: Information about Section 508 of the Act is available at http://www.section508.gov/. The complete text of Section 508 can be accessed at https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh.)

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

The following Section 508 accessibility standards apply to the content or communications material identified in this SOW:

- Functional Performance Criteria
- Electronic Content
- Software
- Support Documentation and Services

Consistent with the revised Section 508 rule effective March 21, 2017, ACL requires contractors to use the Web Content Accessibility Guidelines 2.1 (https://www.w3.org/TR/WCAG21/), and to design and develop digital content and systems for the AA success criteria, conformance to which will meet the current Section 508 criteria for accessibility.

Electronic content must be accessible to HHS acceptance criteria. Checklist for various

formats are available at http://508.hhs.gov/, or from the Section 508 Coordinator listed at https://www.hhs.gov/web/section-508/additional-resources/section-508-contacts/index.html. Materials that are final items for delivery should be accompanied by the appropriate checklist, except upon approval of the Contracting Officer or Representative.

10. Security and Privacy

Before operating any system or workflow that collects, stores, transmits, or processes PII on behalf of ACL, the Contractor shall support ACL in completing required privacy compliance activities, including data inventory, privacy threshold analysis, Privacy Impact Assessment support, records analysis, and review of whether a SORN or other notice is required. The Contractor shall collect only the minimum information necessary for authorized purposes.

All Federal information, including backups, exports, logs containing sensitive data, and data stored on portable or removable media, shall be encrypted at rest and in transit in accordance with HHS policy and approved cryptographic standards. Unencrypted storage of PII on portable/removable media is prohibited unless expressly authorized in writing by ACL

The Contractor shall not input non-public Federal information into third-party generative AI tools unless the tool has appropriate Federal authorization and ACL has approved such use in writing. Any AI-generated output must be reviewed by qualified personnel and shall not be the sole basis for Government decisions.

Applicability. This statement applies whether the entire contract or order (hereafter "contract"), or portion thereof, includes either or both of the following:

Access (Physical or Logical) to Federal Information: A Contractor (and/or any subcontractor) employee will have or given the ability to have, physical or logical (electronic) access to federal information.

Operate a Federal System Containing Information: A Contractor (and/or any subcontractor) will operate a federal system and information technology containing data that directly supports the HHS mission[1]. In addition to the 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

[1]Defined by OMB Circular A-130, as amended, at https://www.whitehouse.gov/omb/circulars_a130_a130trans4/

by the central processing unit of a computer, software, firmware and similar procedures, services (including support services) and related resources.

Contractor Responsibilities. In accordance with the Federal Information Processing Standards Publication (FIPS)199, Standards for Security Categorization of Federal Information and Information Systems, the Contractor (and/or any subcontractor) is responsible for the following:

On behalf of HHS and ACL, protecting federal information and information systems in order to ensure their:

- *Integrity*, which means guarding against improper information modification or destruction, and ensuring information non-repudiation and authenticity;
- *Confidentiality*, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
- *Availability*, which means ensuring timely and reliable access to and use of information.

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

The Contractor (and/or any subcontractor) shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government per clause 52.239-1 of the Federal Acquisition Regulation (FAR)[2].

The Contractor is prohibited from subcontracting to companies to conduct HHS business in which foreign governments that support international terrorism have a "significant interest" per 10 U.S.C. § 2327[3] .

The contractor shall adopt and implement, in consultation with the COR, and the ACL Chief Information Security Officer and Chief Information Officer, the policies, procedures, controls, and standards of the HHS Information Security Program to ensure

[2]FAR 52.239-1, as amended, may be found at https://www.acquisition.gov/sites/default/files/current/far/html/52_233_240.html
[3]More information on subcontracting to foreign governments this may be found at https://www.gpo.gov/fdsys/pkg/USCODE-2011-title10/html/USCODE-2011-title10-subtitleA-partIV-chap137-sec2327.htm

the integrity, confidentiality, and availability of federal information and federal information systems for which the Contractor is responsible under this contract or to which the Contractor may otherwise have access under this contract. The contractor is expected to work in collaboration with the COR, and the ACL Chief Information Security Officer and Chief Information Officer to ensure the security and privacy of systems developed on behalf of ACL. The HHS Information Security and Privacy Policy is available from fisma@hhs.gov. The remainder of this requirement is included as Appendix D, ACL IT Security and Privacy Requirements for the University Centers for Excellence in Developmental Disabilities Education, Research and Service Training and T/TA Project.

AT PROGRAM DATA COLLECTION TRAINING AND TECHNICAL ASSISTANCE (DATA T/TA) TASKS/ACTIVITIES

Project Management and Evaluation (This optional task may be exercised up to one times per year)

1. Annual summative evaluation report on the extent to which T/TA on data analysis and reporting has supported AT Programs in:
    i. Implementing required state-level activities (device demonstrations, device loans, device reutilization, and state financing)
    ii. Implementing required state leadership activities (training, technical assistance, public awareness, information and assistance, coordination and collaboration)
    iii. Achieving compliance with AT Act requirements and federal reporting obligations
    iv. Improving quality and consistency of data collection
    v. Increasing access to and acquisition of AT devices and services for individuals with disabilities
    vi. Demonstrating program impact and outcomes

Knowledge Development, Sharing, and Transfer (This optional task may be exercised up to one times per year)

1. Achieve project goals by providing a progression (e.g., broad based to highly customized) of T/TA knowledge development, sharing and transfer strategies that increase the knowledge base and capacity of AT Program leadership and staff to include:
    a. Developing, maintaining, and redesigning as needed a dynamic, state-of-the-art Website that:
        i. Serves as a primary source of information on data and performance and for AT Programs.
        ii. Is user-friendly, fully accessible, and 508 compliant.

2. Developing and delivering high-quality trainings that include:
    a. Foundational training on AT Act requirements, history, and implementation

   b. Activity-specific training on data reporting (device demonstrations, loans, reutilization, financing, etc.)
   c. Data collection and reporting training

3. Providing rapid response and operational support to AT Programs and ACL staff.

4. Providing individualized, outcome-oriented T/TA to AT Programs in need of assistance to address highly complex matters and circumstances.

5. Facilitating up to two (2) training meetings annually with state and territory AT Program grantees regarding AT Act requirements, reporting requirements, reporting results, data system navigation, and other topics as identified by ACL.

Collaboration (This optional task may be exercised up to one times per year)

1. With the Federal Government
   a. Establish and maintain a partner-focused working relationship with ACL that fosters shared accountability for overall outcomes and responsibility for specific project efforts requiring close collaboration, including federal initiatives involving the AT Programs.
   b. Foster an effective partnership between ACL and AT Programs.
   c. Coordinate, as appropriate, with other ACL programs and federal agencies involved in assistive technology initiatives.
2. With AT Programs
   b. Establish a partner-focused working relationship with AT Programs that facilitates improved program operations, performance, outcomes, and impacts.
   c. Support AT Programs in achieving and maintaining compliance with AT Act statutory and regulatory requirements.
   d. Facilitate collaboration among AT Programs to share promising practices and innovations.

Information Management and Data Systems (This optional task may be exercised up to one times per year)

All Federal information, including backups, exports, logs containing sensitive data, and data stored on portable or removable media, shall be encrypted at rest and in transit in accordance with HHS policy and approved cryptographic standards. Unencrypted storage of PII on portable/removable media is prohibited unless expressly authorized in writing by ACL.

The Contractor shall provide comprehensive data collection, reporting, and dissemination services to support AT Program federal reporting requirements and public access to AT Program data:

1. AT Data Collection and Reporting System Operations
   a. Support the maintenance of the AT Reporting System (ATRS) or equivalent system to remain operational for receipt of AT Annual Progress Reports (AT APRs) and State Plans for Assistive Technology (State Plans for AT).
   b. Ensure the AT APR data collection period operates annually from October through December to allow all 56 state and territory AT Programs to submit their AT APR data.

c. Ensure the State Plan for AT data collection operates on a three-year cycle, opening each August for a 60-day submission period.
d. Develop and implement code changes to the existing AT APR, Day-to-Day module, and State Plan for AT to align the reporting system with approved OMB information collection instruments.
e. Technical assistance and support for the ATRS data collection instrument for 56 state and territory AT Annual Progress Reports that comply with OMB approval requirements.
f. Technical assistance and support for the ATRS data collection instrument for 56 state and territory AT State Plans that comply with OMB approval requirements.
g. Provide a day-to-day data tracking system as an option that state and territory AT Programs can use to record service delivery data that aggregates to populate the AT APR and State Plan.
h. Support data analysis and reporting for the individual 56 state and territory AT Annual Progress Reports.
i. Support data analysis and reporting for the individual 56 state and territory AT State Plans.
j. Review 56 state and territory AT Annual Progress Reports for data validation and completion.
k. Review 56 state and territory AT State Plans for data validation and completion.
l. Serve as primary point of contact for AT Program State Plan and Annual Progress reporting questions and technical assistance.
m. Provide training, technical assistance, and work with state and territory AT Program lead agencies and implementing entities to resolve data validation and/or incomplete data field items.
n. Coordinate semiannual meetings with ACL and all subcontractors and quarterly meetings with subcontractors as needed.
o. Meet regularly with, coordinate, and oversee all subcontractor reporting and deliverables.

2. Data Transfer and System Integration
    a. Transmit all historical state and territory AT data into any AT Reporting System in the ACL environment as directed.
    b. Provide ACL staff with technical assistance to support internal resolution of any development, deployment, and operational issues with ACL AT Reporting System implementation.
    c. Support transmittal of all AT APR and State Plan data to the ATRS and public-facing CATADA website.

3. Public Data Dissemination - CATADA.info Website
    a. Maintain a searchable online public database that includes the 56 state and territory AT APR data and state and territory AT Plans at CATADA.info or equivalent public-facing platform.
    b. Maintain, update, and troubleshoot the CATADA.info website to ensure continuous operation and accessibility.
    c. Continually update individual AT Program pages with current logos and accurate program information.
    d. Post new three-year State Plans for AT within 30 days of receipt and validation.
    e. Update the CATADA.info website with state and territory AT APRs within 60 days of data validation.
    f. Review APR data in Excel files for data errors and consistency prior to posting.

g. Brand and upload individual state and aggregate HTML files.
h. Upload APR data to Google Sheets or equivalent platform for public access.
i. Spot-check APR data viewable on CATADA for technical errors and compare viewable data to raw data to ensure accuracy.

4. Annual AT Report to Congress
   a. Develop, remediate, finalize, and post the annual AT Report to Congress that includes anecdotes, public awareness stories, and a special feature section.
   b. Review hundreds of anecdotes submitted by AT Programs and select representative anecdotes for sections on device demonstrations, device loans, device reuse, state financing, and public awareness.
   c. Edit selected anecdotes and conduct follow-up with AT Programs as necessary to ensure accuracy and completeness.
   d. Coordinate with ACL on report structure, content, and timeline to meet Congressional reporting deadlines.
   e. Ensure the final report is accessible, 508-compliant, and professionally formatted.

5. CATADA Catalogue of Initiatives
   a. Maintain the CATADA Catalogue of Initiatives as a repository of field-generated initiatives submitted by State AT Program grantees and their contractors/partners. b. Review hundreds of state improvement outcomes and innovations submitted by AT Programs annually. c. Edit anecdotes and populate the Catalogue of Initiatives with impactful and innovative AT initiatives from programs across the country. d. Organize the Catalogue by categories (e.g., device demonstrations, financing, reutilization, public awareness) to facilitate searchability. e. Update the Catalogue regularly to reflect current and emerging practices.

6. State-Level Analysis and Reporting
   a. Analyze the 56 state and territory AT Plans to identify themes, partnerships, and emerging opportunities.
   b. Draft and finalize reports on AT State Plans that highlight themes, partnerships, and emerging opportunities for ACL review.
   c. Provide data analysis and custom reports as requested by ACL in accordance with ACL format and guidelines.

7. System Security, Privacy, and Accessibility Requirements
   a. Provide all technology-related activities in this contract in accordance with the security and privacy requirements established in Attachment A, ACL Security and Privacy Requirements.
   b. Ensure all data systems and websites comply with Section 508 of the Rehabilitation Act and Web Content Accessibility Guidelines (WCAG) 2.1 Level AA standards.
   c. Maintain compliance with HHS Binding Operational Directive (BOD) 18-01 including Email Security and Web Security requirements.
   d. Configure all internet-facing mail servers to offer STARTTLS.
   e. Configure all second-level domains to have valid SPF/DMARC records.
   f. Ensure Secure Sockets Layer (SSL) v2 and SSLv3 are disabled on mail and web servers.
   g. Ensure 3DES and RC4 ciphers are disabled on mail and web servers.
   h. Ensure all publicly accessible federal websites and web services provide service through a secure connection (HTTPS-only, with HSTS).

i. Protect the integrity, confidentiality, and availability of federal information and federal information systems in accordance with FIPS 199 Standards for Security Categorization of Federal Information and Information Systems

C.3 INFORMATION SECURITY AND/OR PHYSICAL ACCESS SECURITY REQUIREMENTS

Important Note to Contractor: In the event of a discrepancy between the following language and included HHSAR clauses, the HHSAR clauses take precedence.

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 HHS mission. In addition to the Federal Acquisition Regulation (FAR) Subpart 2.1 definition of "information technology" (IT), the term as used in this section includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources.
   b. **Safeguarding Information and Information Systems.** All government information and information systems must be protected in accordance with HHS 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 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 ISSO, CISO, OpDiv 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:** [X] Low [ ] 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 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 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 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/OpDiv 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, HHS uses a privacy analysis process to assess the risks associated with HHS'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 HHS 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 or not 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 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 policies. Unauthorized disclosure of information will be subject to the HHS 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-21-07, Completing the Transition to Internet Protocol Version 6 (1Pv6) available at https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-07.pdf

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, 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.

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 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 OpDiv-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.

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.

vi. **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 OpDiv non-disclosure agreement. 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/OpDiv 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 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*.

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 OpDiv 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)/ 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)*, 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 approved notifications to affected individuals.

iii. Report all suspected and confirmed information security and privacy incidents and breaches to the OpDiv Incident Response Team (IRT), COR, CO, OpDiv 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 OpDiv 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/OpDiv and 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.

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 HSPD-12 policy; and *Executive Order 13467, Part 1 §1.2.*

Note to the Requiring Activity Representative: *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 *[OpDiv Specific timeline]* of the effective date of this contract. Any revisions to the roster as a result of staffing changes must be submitted within *[OpDiv Specific timeline]* of the change. The COR will notify the Contractor of the appropriate level of investigation required for each staff member.

If the employee is filling a new position, the Contractor 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, 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 Guide (2012).
   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 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 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 policies.

f. The Contractor (and/or any subcontractor) must perform and document the actions identified in the Contractor Employee Separation Checklist when an employee terminates work under this contract upon 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* policies and must not dispose of any records unless authorized by HHS.
   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 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 DHS HVA Control Overlay in addition to the above requirements.

C.4 PROCUREMENTS INVOLVING GOVERNMENT INFORMATION PROCESSED ON GOCO OR COCO SYSTEMS

Important Note to Contractor: In the event of a discrepancy between the following language and included HHSAR clauses, the HHSAR clauses take precedence.

1. Security Requirements for GOCO and COCO Resources
   a. **Federal Policies.** The Contractor (and/or any subcontractor) must comply with applicable federal laws and HHS policies that include, but are not limited to,

the *HHS Information Security and Privacy Policy (IS2P)*; *Federal Information Security Modernization Act (FISMA) of 2014, (44 U.S.C. 101)*; National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, latest revision, *Security and Privacy Controls for 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. **Assessment and Authorization (A&A)**. A valid authority to operate (ATO) certifies that the Contractor's information system meets the contract's requirements to protect the agency data. If the system under this contract does not have a valid ATO, the Contractor (and/or any subcontractor) must work with the agency and supply the deliverables required to complete the ATO within the specified timeline(s). The Contractor must conduct the A&A requirements in accordance with *HHS IS2P,* NIST SP 800-37, *Guide for Applying the Risk Management Framework to Information Systems: A Security Life Cycle Approach* (latest revision), NIST SP 800-53B, *Control Baselines for Information Systems and Organizations*, and the NIST SP 800-53A (latest revision).

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

i. **A&A Package Deliverables** - The Contractor (and/or any subcontractor) must provide an A&A package to the CO and/or COR. The following A&A deliverables are required to complete the A&A package:

- **System Security Plan (SSP)** - due *[insert specific timeline, process, and format after contract award]*. The SSP must comply with the NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, the Federal Information Processing Standard (FIPS) 200, *Recommended Security Controls for Information Systems*, and NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* applicable baseline requirements, and other applicable NIST guidance as well as HHS and *[OpDiv]* policies and other guidance. The SSP must be consistent with and detail the approach to IT security contained in the Contractor's bid or proposal that resulted in the award of this contract. The SSP must provide an overview of the system environment and security requirements to protect the information system as well as describe all applicable security controls in place or planned for meeting those requirements. It should provide a structured process for planning adequate, cost-effective security protection for a system. The Contractor must review and update the SSP at least ***annually*** thereafter and if requested, provide a copy of the updated SSP.

- **Security Assessment Plan/Report (SAP/SAR)** - due *[insert specific timeline, process and format after contract award.]* The security assessment must be conducted by assessor and be consistent with NIST SP 800-53A, NIST SP 800-30, and HHS and OpDiv policies. The assessor will document the assessment results in the SAR.

  Thereafter, the Contractor, in coordination with ACL must conduct in the assessment of the security controls and update the SAR at least ***annually***. A copy of the updated SAR should be provided if requested.
- **Independent Assessment -** The Contractor (and/or subcontractor) must have an independent third-party validate the security and privacy controls in place for the system(s) commensurate with the risk levels per NIST SP 800-53B. The independent third party must review and analyze the Security Authorization package, and report on technical, operational, and management level deficiencies as outlined in NIST SP 800-53. The Contractor must address all *"high"* deficiencies before submitting the package to the Government for acceptance and document all remaining deficiencies in a system Plan of Actions and Milestones (POA&M).
- **POA&M** -All critical-risk weaknesses must be mitigated within **15 days**, high-risk weaknesses must be mitigated within **30 days**, medium weaknesses must be mitigated within **90 days**, and low weaknesses must be mitigated within **180 days**,from the date the weaknesses are formally identified and documented. ACL will determine the risk rating of vulnerabilities. Identified risks stemming from deficiencies related to the security control baseline implementation, assessment, continuous monitoring, vulnerability scanning, flaws and security defect in a system (that require to create a patch for remediation), and other security reviews and sources, as documented in the SAR, must be documented and tracked by the Contractor for mitigation in the POA&M document consistent with the HHS Standard for Plan of Action and Milestones and OpDiv policies. Depending on the severity of the risks, ACL may require designated POA&M weaknesses to be remediated before an ATO is issued. Thereafter, continue to remediate weaknesses throughout the contract. The POA&M document must be updated at least **quarterly.**
- **Contingency Plan and Contingency Plan Test** - The Contingency Plan must be developed in accordance with NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems*, and be consistent with HHS and OpDiv policies. Upon acceptance by the System Owner, the Contractor, in coordination

with the System Owner, must test the Contingency Plan and prepare a Contingency Plan Test Report that includes the test results, lessons learned and any action items that need to be addressed. Thereafter, the Contractor must update and test the Contingency Plan at least ***annually***.

- **E-Authentication Questionnaire** - The contractor (and/or any subcontractor) must collaborate with government personnel to ensure that the E-Authentication requirements are implemented in accordance with OMB 04-04 and NIST SP 800-63 B.

  Based on the level of assurance determined by the E-Auth, the Contractor (and/or subcontractor) must ensure appropriate authentication to the system, including remote authentication, is in-place in accordance with the assurance level determined by the E-Auth (when required) in accordance with HHS *Guidance for Selection of e-Authentication Assurance Levels* and any other applicable HHS policies.

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

iii. **Annual Assessment/Penetration (Pen) Test -** Assess the system security and privacy controls (or ensure an assessment of the controls is conducted) at least annually to determine the implemented security and privacy controls are operating as intended and producing the desired results (this involves penetration testing conducted by the agency or independent third-party) In addition, review all relevant A&A documentation (SSP, POA&M, Contingency Plan, etc.) and provide updates by specified due date.

iv. **Asset Management -** Using any available Security Content Automation Protocol (SCAP)-compliant automated tools for active/passive scans, provide an inventory of all information technology (IT) assets for hardware and software, (computers, servers, routers, databases, operating systems, etc.) that are processing HHS-owned information/data. It is anticipated that this inventory information will be required to be produced. IT asset inventory information must include IP address, machine name, operating system level, security patch level, and SCAP-compliant format information. The contractor must maintain a capability to provide an inventory of 100% of its IT assets using SCAP-compliant automated tools in accordance with the *HHS Policy for Information Technology Asset Management (ITAM)* and any other applicable HHS policy.

v. **Configuration Management -** Use available SCAP-compliant automated tools as per NIST IR 7511 and *HHS Minimum Security Configurations Standards Guidance* to scan all IT assets, including but not limited to: computers, servers, routers, databases, operating systems, application, etc., that store and process government information. Provide scan reports to HHS upon request. The contractor must maintain a capability to provide security configuration compliance information for 100% of its IT assets using SCAP-compliant automated tools.

vi. **Vulnerability Management -** Contractors must actively manage system vulnerabilities using automated tools and technologies where practicable and in accordance with *HHS Policy for Vulnerability Management*. Automated tools must be compliant with NIST-specified SCAP standards for vulnerability identification and management. The contractor must maintain a capability to provide security vulnerability scanning information for 100% of IT assets using SCAP-compliant automated tools and report to the agency at least *[insert specific timeframe]*.

vii. **Patching and Vulnerability Remediation -** Install vendor released security patches and remediate critical and high vulnerabilities in systems processing government information in an expedited manner, within vendor and agency specified timeframes.

viii. **Secure Coding -** Follow the *HHS Policy for Software Development Secure Coding Practices* and 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.

ix. **Boundary Protection -** The contractor must ensure that government information, other than unrestricted information, being transmitted from federal government entities to external entities is routed through a Trusted Internet Connection (TIC).

c. **Government Access for Security Assessment**. In addition to the Inspection Clause in the contract, the Contractor (and/or any subcontractor) must 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.

d. **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 if it impact enterprise-wide systems and services, or by the OpDiv CISO if it impact only the OpDiv). The contractor must retire and/or upgrade all software/systems that have reached end-of-life in accordance with *HHS End of Life Operating Systems, Software and Application Policy*.

e. **Desktops, Laptops, and Other Computing Devices Required for Use by the Contractor**. The Contractor (and/or any subcontractor) must 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 encryption standard and current FIPS 140 validation certificate from the NIST CMVP.
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;
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 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.

f. **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.

g. **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.

C.5 OTHER IT PROCUREMENTS

Important Note to Contractor: In the event of a discrepancy between the following language and included HHSAR clauses, the HHSAR clauses take precedence.

1. Hardware Procurements

   a. **Card Readers**. The Contractor (and/or any subcontractor) must include Federal Information Processing Standard (FIPS) 201-compliant smart card readers (referred to as LACS Transparent Readers) with the purchase of servers, printers, desktops, and laptops.
   b. **Mobile Devices**. The contractor must follow NIST 800-124, Rev. 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise* and comply with Public Law 115-232 § 889, when purchasing mobile devices that process or store HHS data.

2. Non-Commercial and Open Source Computer Software Procurements

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.

3. 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 must consult the guidelines from NIST SP 800-160 volume 1, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, NIST SP 800-160 volume 2, *Systems*

Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, and NIST SP 800-53 to implement security during the development of all applications and throughout the life cycle stages of software development.

c. 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, the Open Web Application Security Project (OWASP), System Admin, Audit, Network and Security (SANS), and the *HHS Policy for Software Development Secure Coding Practices* that will limit system software vulnerability exploits.
d. 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.
e. The contractor must, at a minimum, segregate physically or logically, all test and development systems from production systems as applicable in accordance with the HHS *Standard for Segregation of Dev/Test Environments from Production*.
f. 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.

4. Physical Access to Government Controlled Facilities

Additionally, due to the COVID-19 Epidemic of 2020 (Effective as of March 30, 2020), The below contract language must be included in all COVID-19 contract actions until such time the HHS Secretary makes a determination to issue rated contracts related to items used for allowing HHS employees/contractors to physically use and/or operate in HHS facilities and spaces.

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

C.6 ADDITIONAL HSPD-12 REQUIREMENTS

Important Note to Contractor: In the event of a discrepancy between the following language and included HHSAR clauses, the HHSAR clauses take precedence.

To perform the work specified herein, contractor personnel will require access to proprietary,

privacy protected and/or sensitive data, regular access to HHS-controlled facilities and/or access to HHS information systems. In addition to requirements stated elsewhere in this contract, the contractor shall comply with the following.

Contractor personnel subject to HSPD-12 credentialing requirements may not begin work requiring access to HHS facilities, information or information systems until codified credentialing standards are met and the HSPD12 badges have been issued.

The minimum Government investigation to receive an HSPD-12 PIV Credential is a Tier 1 (NACI), which consists of searches of records covering specific areas of a person's background during the past five years. The minimum Government investigation to receive Elevated Privilege (any access beyond normal email or data entry) is a Tier 4 (BI High Risk Public Trust).

The contractor must comply with the instructions and timeframes provided by the Contracting Officer's Representative (COR) regarding the handling of the security requirements specified in this section. Typically, each employee must submit at a minimum: a completed OF-306; a current resume; and a completed HHS 828 form. Additional requirements may apply to Foreign National Applicants who will follow a slightly different level of initial checks. Contractors should ensure that the employees whose names they submit have a reasonable chance for access approval. In some cases, employees with existing background investigations commensurate with sensitivity designations will expedite performance. Inquiries, including requests for forms and assistance, should be directed to the COR.

Typically, the Government investigates personnel at no cost to the contractor, but the expense of multiple investigations for the same position is difficult to justify. Consequently, multiple investigations for the same position may, at the Contracting Officer's discretion, justify reduction(s) in the contract price of no more than the cost of the extra investigation(s).

After final acceptance of the work specified herein or any employee departure, the contractor shall follow the COR's instruction on the return of all identification badges, building access cards, Government Furnished Equipment, Government Furnished Data and Government Furnished Property (GFE/GFD/GFP) as applicable.

HHS reserves the right to suspend or withdraw access at any time for any reason.

Language similar to this Security section shall be included in any subcontracts which require access to proprietary, privacy protected and/or sensitive data, regular access to HHS-controlled facilities and/or access to HHS information systems.

C.7 HHS DIGITAL ACCESSIBILITY CONFORMANCE STANDARDS – INFORMATION AND COMMUNICATION TECHNOLOGY

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.

All products, platforms and services delivered as part of this contract that are ICT, or contain ICT, must conform to all HHS digital accessibility conformance standards identified in the HHS Digital Accessibility Conformance Checklists. The standards include the Revised 508 Standards, which are located at 36 C.F.R. § 1194.1 & Apps. A, B, & C, and available at https://www.access-board.gov/ict/.

All requirements are applicable to support services and documentation deliverables. 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.

The standards listed below apply to all functionality of the supplies, products, platforms, information, documentation, training, and services that are part of this contract.

- 508 Chapter 2:
    - E205 Electronic Content
    - E207 Software
    - E208 Support Documentation and Services
- 255 Chapter 2:
    - C203 Electronic Content
    - C205 Software
    - C206 Support Documentation and Services
- Chapter 3: Functional Performance Criteria
- Chapter 5: Software
- Chapter 6: Support Services and Documentation Requirements

Prior to acceptance of deliverables, the contractor must demonstrate conformance to the HHS digital accessibility conformance standards. The government reserves the right to perform testing on required ICT items to validate the offeror's digital accessibility and Section 508 conformance claims. If the government determines that conformance does not meet the HHS digital accessibility conformance standards, the government shall, at its option, require the contractor to remediate the item, at no additional cost to the government, to align with the HHS digital accessibility conformance standards prior to acceptance.

C.8 QUALITY ASSURANCE SURVEILLANCE PLAN (QASP)

The Government intends to utilize a Quality Assurance Surveillance Plan (QASP) to monitor the quality of the Contractor's performance. The oversight provided for in the contract and in the

QASP will help to ensure that service levels reach and maintain the required levels throughout the contract term. Further, the QASP provides the COR with a proactive way to avoid unacceptable or deficient performance, and provides verifiable input for the Contractor Performance Assessment Reporting System (CPARS). The QASP may be updated by modification to the contract.

Quality Assurance Surveillance Plan (QASP)

PWS Section	Service / Task	Performance Standard	Acceptable Quality Level (AQL)	Method of Surveillance	Consequence of Nonperformance
3.1(a)-(b)	Project planning and advisory structure	Required planning documents and advisory committee functions are established, maintained, and used to guide contract implementation and continuous improvement.	90% on-time for recurring 3.1 planning or advisory submissions; required committee maintained and meetings held as required; 90% completeness of sampled documentation.	Document review; periodic inspection by COR.	Written deficiency notice; contractor response or corrective action if issues recur.
3.1(c)-(d)	Performance monitoring, monthly reporting, and dashboard oversight	The contractor regularly monitors performance, submits required monthly reporting, and maintains an accessible dashboard or comparable tool that supports transparency, risk identification, and course correction.	90% of recurring reports submitted on time; 90% completeness of sampled content; dashboard or comparable tool available 98% of the time, excluding approved maintenance; material data issues corrected within COR-established timeframe.	Document review; dashboard review; periodic inspection; random monitoring.	Written deficiency notice; targeted corrective action or CAP for recurring reporting or system issues.
3.1(e)	Evaluation and continuous quality improvement	The contractor conducts ongoing formative assessment and an annual summative evaluation and uses the results to improve service quality, efficiency, and outcomes.	90% of recurring assessment products submitted on time; annual evaluation submitted by required due date; 90% coverage of required evaluation domains.	Document review; 100% inspection of annual evaluation by COR.	Written deficiency notice; CAP if evaluation products are late, materially incomplete, or not used for improvement.
3.2	UCEDD website, training, and broad-based T/TA delivery	The contractor maintains accessible website resources and delivers required training, orientation, leadership development, and peer-learning activities consistent with the approved work plan.	90% of scheduled activities delivered; website available 98% of the time; 100% accessibility at delivery; at least 80% participant satisfaction or reported knowledge, skill, or confidence gain where measured.	Periodic inspection; customer feedback; attendance review; random monitoring; accessibility review.	Written deficiency notice; remediation plan for repeated service or website deficiencies.
3.2	Targeted consultation, peer support, dissemination, and impact communication	The contractor provides practical consultation, peer connection, dissemination support, and communication tools that help UCEDDs address complex issues and communicate impact.	90% of requests addressed within agreed timeframe; 90% of required tools or support products delivered on time; at least 75% of participating UCEDDs demonstrate improved dissemination, outreach, or use	Document review; customer feedback; periodic inspection.	Written deficiency notice; targeted corrective action for recurring timeliness or service-quality

PWS Section	Service / Task	Performance Standard	Acceptable Quality Level (AQL)	Method of Surveillance	Consequence of Nonperformance
			of support provided, where measured.		problems.
3.2	Impact measurement strategy and UCEDD Impact Portfolio	The contractor maintains an integrated impact measurement approach and produces an accessible annual impact portfolio or comparable product suitable for ACL, UCEDDs, and other stakeholders, as appropriate.	Annual portfolio submitted by required due date; 90% completeness across sampled required elements; 75% or more of participating UCEDDs represented through current entries, examples, or updates.	100% inspection of annual portfolio; document review; periodic inspection.	Written deficiency notice; CAP for repeated lateness or material omissions.
3.3	UCEDD coordination and stakeholder engagement	The contractor maintains responsive working relationships with UCEDDs and key partners and facilitates peer exchange, shared learning, and coordinated action.	90% of planned coordination activities completed; annual documentation shows active engagement and support for collaboration, problem-solving, or issue resolution; at least 75% of participating UCEDDs demonstrate increased coordination or use of shared practices, where measured.	Document review; periodic inspection; customer feedback.	Written deficiency notice; engagement strategy revision or CAP if coordination performance is weak.
3.4	UCEDD information management, reporting support, and public-facing tools	The contractor maintains a reliable, secure, and accessible system for required UCEDD reporting, data support, training, and public-facing information functions.	99.5% uptime during critical reporting periods; 100% compliance with security and accessibility requirements; 90% of standard support items or reports completed within agreed timeframe.	Periodic inspection; random monitoring; security and accessibility review; document review.	Written deficiency notice; CAP for systemic issues; immediate notification for security incidents.
4.1-4.3	AT Program management, T/TA delivery, and collaboration	The contractor provides annual evaluation, accessible website support, training, rapid response, individualized assistance, and collaboration with ACL, AT Programs, and other partners.	90% of scheduled activities delivered; annual evaluation submitted by required due date; 90% of requests addressed within agreed timeframe; at least 80% customer satisfaction or reported usefulness where measured.	Document review; customer feedback; periodic inspection.	Written deficiency notice; remediation plan or CAP for repeated deficiencies.
4.4	AT data systems, reporting operations, and technical support	The contractor maintains AT reporting systems and technical support for annual progress reports, state plans, data validation, and related user assistance.	99.5% uptime during submission windows; 95% of required system support actions completed within agreed timeframes; 98% sampled data accuracy on outputs; material system-caused errors corrected promptly.	Periodic inspection; random monitoring; document review.	Written deficiency notice; CAP for recurring system or data problems; immediate notification if critical outage occurs.
4.4	AT public dissemination and required reporting products	The contractor maintains CATADA.info or equivalent public-facing tools and delivers required public	95% of recurring updates or postings completed on time; 98% sampled data accuracy; major annual reports submitted	Periodic inspection; random monitoring;	Written deficiency notice; remediation required; CAP

PWS Section	Service / Task	Performance Standard	Acceptable Quality Level (AQL)	Method of Surveillance	Consequence of Nonperformance
		updates, annual reports, and analysis products in accessible formats.	by required deadline; 100% accessibility at delivery.	100% inspection of major annual reports by COR.	for repeated late postings, data issues, or inaccessible deliverables.
All Sections	Accessibility and Section 508 compliance	All digital deliverables, websites, and systems comply with applicable Section 508 and WCAG 2.1 Level AA requirements.	100% compliance at delivery; accessibility defects remediated within COR-established timeframe.	Accessibility review; 100% inspection of final digital deliverables; periodic inspection.	Remediation at contractor expense; written deficiency notice; possible additional remedies for persistent noncompliance.
All Sections	Security, privacy, and subcontractor performance	The contractor protects federal information and systems, reports incidents timely, and remains fully responsible for subcontractor performance.	100% security and privacy compliance; incidents reported within 1 hour of discovery; subcontractor performance meets applicable standards for assigned work.	Security review; document review; periodic inspection; random monitoring.	Immediate notice to COR and CO; CAP; same remedies apply to subcontractor failures.

SECTION D - Packaging and Marking

D.1 PACKAGING AND MARKING

All deliverables shall be delivered to the Contracting Officer's Representative (COR) identified in Section G and shall be marked as follows:

1. Name and address of the Contractor;
2. Contract Number;
3. Description of item contained therein; and
4. Consignee's name and address.

D.2 PAYMENT OF POSTAGE AND FEES

All postage and fees related to submitting information including forms, reports, etc. to the Contracting Officer or COR shall be paid by the Contractor.

SECTION E - Inspection and Acceptance

E.1 INSPECTION AND ACCEPTANCE

Pursuant to the appropriate inspection clause, all work described in Section C to be delivered under this contract is subject to final inspection and acceptance by an authorized representative of the Government. The authorized representative of the Government is the Contracting Officer's Representative (COR), who is responsible for inspection and acceptance of all services, materials, or supplies to be provided by the Contractor.

E.1.1 Inspection and Acceptance Criteria

Final inspection and acceptance of all work performed, reports and other deliverables will be performed at the place of delivery by the COR.

E.1.2 General Acceptance Criteria

General quality measures, as set forth below, will be applied to each work product received from the Contractor under this Statement of Work.

- Accuracy - Work Products shall be accurate in presentation, technical content, and adherence to accepted elements of style.
- Clarity - Work Products shall be clear and concise. Any/all diagrams shall be easy to understand and be relevant to the supporting narrative.
- Consistency to Requirements - All work products must satisfy the requirements of this Statement of Work.
- File Editing - All text and diagrammatic files shall be editable by the Government.
- Format - Work Products shall be submitted in hard copy and electronic copy. The electronic copy must be in a format as indicated in the Deliverables Table.

SECTION F - Deliveries or Performance

F.1 PERIOD OF PERFORMANCE – Severable Services

The period of performance shall be for a base period of 12 months, with four (4) 12 month option periods, as follows:

Base Period	September 30, 2026 – September 29, 2027
Option Period 1	September 30, 2027 – September 29, 2028
Option Period 2	September 30, 2028 – September 29, 2029
Option Period 3	September 30, 2029 – September 29, 2030
Option Period 4	September 30, 2030 – September 29, 2031

Option periods may be exercised in accordance with FAR Clause 52.217-9 entitled "Option to Extend the Term of the Contract."

F.2 PLACE OF PERFORMANCE

Work will be performed at the Contractor's primary place of performance at:
CONTRACTOR'S PRIMARY PLACE OF PERFORMANCE, but the contractor is not prohibited from allowing its employees to telework in accordance with the contractor's policies if the work and required level of performance can be completed successfully in accordance with the contract requirements. The Contractor shall coordinate employee telework in advance with the Contracting Officer's Representative.

F.3 REPORT(S)/DELIVERABLES AND DELIVERY SCHEDULE

In fulfillment of this effort, the Contractor shall provide the following deliverables. All deliverables shall be submitted to the COR, unless otherwise agreed upon. Unless otherwise specified, the Government will have a maximum of ten business days from the day the draft deliverable is received to review the document, provide comments back to the contractor, approve or disapprove the deliverable(s). The contractor will also have a maximum of ten business days from the day comments are received to incorporate all changes and submit the final deliverable to the Government. All days identified below are intended to be business days unless otherwise specified.

PWS Section / Objective	Deliverable	Due Date / Frequency
3.1(a) Strategic Planning, Logic Model, and Performance Measurement and Evaluation	Initial 5-year strategic plan, logic model, and performance measurement and evaluation matrix for delivery of T/TA	Within 60 calendar days after contract start date

Matrix		
3.1(a) Strategic Planning, Logic Model, and Performance Measurement and Evaluation Matrix	Annual update to the 5-year strategic plan, logic model, and performance measurement and evaluation matrix	By October 30 of each Option Period
3.1(a) Strategic Planning, Logic Model, and Performance Measurement and Evaluation Matrix	Interim revisions to strategic plan, logic model, and/or performance measurement and evaluation matrix to reflect federal priorities or COR direction	As directed by the COR
3.1(b) Project Advisory Committee	Project Advisory Committee charter, proposed membership, and meeting schedule	Within 60 calendar days after contract start date
3.1(b) Project Advisory Committee	Project Advisory Committee meeting materials, summaries, and recommendations	At least semi-annually; summaries due within 10 business days after each meeting
3.1(c) Ongoing Performance Monitoring and Reporting	Monthly report to the COR summarizing emerging and recurring T/TA needs, T/TA provided, progress toward goals/objectives/outputs/outcomes, key risks/barriers, mitigation strategies, and recommended adjustments	Monthly; due on the 15th day of the following month
3.1(d) T/TA Services Performance Dashboard	Dashboard design and implementation plan	Within 60 calendar days after contract start date
3.1(d) T/TA Services Performance	Initial operational, secure, real-time, Section 508-compliant interactive T/TA Services Performance Dashboard	Within 120 calendar days after

Dashboard		contract start date
3.1(d) T/TA Services Performance Dashboard	Dashboard updates, maintenance, and performance/data refresh	Continuous; updated in real time or as data become available
3.1(d) T/TA Services Performance Dashboard	Dashboard findings, trends, and performance insights shared with UCEDD leadership through webinars, written summaries, and/or network meetings	Quarterly, or as directed by the COR
3.1(e) Evaluation and Continuous Quality Improvement - Formative Assessment	Monthly formative assessment findings on progress of project activities, service quality, efficiency, and progress toward contract outcomes	Monthly; due on the 15th day of the following month
3.1(e) Evaluation and Continuous Quality Improvement - Summative Evaluation	Annual summative assessment to OIDD on the extent to which the T/TA improved UCEDD capacity, performance, data quality/usefulness, leadership, and outcomes for individuals with I/DD and their families	By September 30 of the Base Year and each Option Period
3.2 Website	Website continuity/transition plan for the T/TA website, including content structure and navigation design for COR approval	Within 30 calendar days after contract start date
3.2 Website	Modern, dynamic, searchable, fully accessible, Section 508-compliant T/TA website operational	Within 90 calendar days after contract start date; continuous operation thereafter
3.2 Website / Resource Library	Curated, searchable, continuously updated library of tiered resources, tools, peer examples, impact materials, and T/TA opportunities	Ongoing; updated continuously
3.2 Website / Resource	Annual comprehensive review of website content, resource library, outdated material archive, and content prioritization	By September

Library	informed by analytics, user feedback, and T/TA demand trends	30 annually
3.2 Training and Peer Learning	Annual training and peer-learning plan covering director orientation, leadership development, disability-specific/current-emerging issues, UCEDD infrastructure/operations/compliance, peer-learning forums, and NIRS/PPR data use beyond compliance reporting	Within 90 calendar days after contract start date; updated annually by October 30
3.2 Training and Peer Learning	Comprehensive orientation for UCEDD Directors	Annually, or more frequently as needed for onboarding/ new directors
3.2 Training and Peer Learning	Leadership development curricula and skill-building opportunities for UCEDD staff and emerging leaders	At least semi-annually, or as approved by the COR
3.2 Training and Peer Learning	Disability-specific and topic-specific training responsive to current and emerging issues	At least semi-annually, or as approved by the COR
3.2 Training and Peer Learning	Training to strengthen UCEDD infrastructure, operations, compliance, planning, and performance	At least semi-annually, or as approved by the COR
3.2 Training and Peer Learning	Regional, cross-network, and topic-based peer-learning forums	Quarterly, or as approved by the COR
3.2 Training and Peer Learning	Training on use of NIRS/PPR and related performance data for strategic communications, visibility, impact messaging, and decision-making beyond compliance reporting	Annually, with updates as needed
3.2 Expert Analysis and Responsive Consultation	High-quality expert analysis, decision-support resources, peer examples, and responsive consultation addressing emerging policy, programmatic, operational, and disability-related issues	Quarterly, or as needed and approved by the COR
3.2	Plan and operating approach for individualized, outcome-	Within 90

Individualized T/TA and Peer Connection Strategies	oriented T/TA and peer connection strategies	calendar days after contract start date
3.2 Individualized T/TA and Peer Connection Strategies	Cadre/roster of proven experts available to support UCEDD leadership, faculty, staff, and CAC members	Initial roster within 90 calendar days after contract start date; updated quarterly
3.2 Individualized T/TA and Peer Connection Strategies	Formal peer mentorship approach for UCEDD Directors, including support for new Directors and those facing complex leadership or operational challenges	Within 120 calendar days after contract start date; ongoing thereafter
3.2 Individualized T/TA and Peer Connection Strategies	Site visits, peer consultation, and structured learning opportunities to observe scalable programs, effective practices, and successful operational approaches	As requested, approved, and scheduled
3.2 Dissemination Capacity and Public Awareness	Dissemination and strategic communications T/TA plan, including plain language, accessible dissemination, digital engagement, media relations, audience-centered message development, and evidence-informed impact communication	Within 120 calendar days after contract start date; updated annually
3.2 Dissemination Capacity and Public Awareness	Tools, templates, and guidance to support data-informed messaging, modern dissemination practices, national messaging, replicable dissemination/public awareness approaches, and communication of impact beyond compliance reporting	Initial package within 150 calendar days after contract start date; updated annually
3.2 Dissemination Capacity and Public Awareness	Targeted T/TA to UCEDDs needing additional support to strengthen dissemination effectiveness and communicate impact for people with I/DD and their families	Ongoing; summarized semi-annually

3.2 Impact Measurement and Data Strategy	Integrated impact measurement framework or comparable approach connecting federal investment, UCEDD activities/partnerships, outputs, outcomes, and demonstrated impact	Within 120 calendar days after contract start date
3.2 Impact Measurement and Data Strategy	Comprehensive UCEDD Impact Portfolio framework, data fields, and methodology	Within 150 calendar days after contract start date
3.2 Impact Measurement and Data Strategy	Annual UCEDD Impact Portfolio, including accessible presentations of findings, quantified impact where feasible, promising practices, replicable models, return on federal investment, and annual updates	By September 30 of the Base Year and each Option Period
3.3 Coordination with UCEDDs	Coordination and engagement plan for the UCEDD Network addressing communication, needs identification, timely problem-solving, peer exchange, shared learning, cross-center problem-solving, and support across multiple funding streams/institutional contexts	Within 90 calendar days after contract start date
3.3 Coordination with UCEDDs	Documentation/summaries of coordination activities with UCEDDs, including needs identified, support provided, peer exchange efforts, and actions to strengthen performance, outcomes, scalability, and collective impact	Semi-annually
3.3 Coordination with Other Key Stakeholders	Stakeholder coordination plan addressing DD Act partners, Independent Living programs/centers, federal and non-federal partners, and cross-system partners such as VR, education, healthcare, aging services, IDEA-funded systems, and workforce systems under WIOA	Within 90 calendar days after contract start date
3.3 Coordination with Other Key Stakeholders	Documentation/summaries of regional, national, and topic-based engagement opportunities promoting cross-state/cross-territory collaboration, peer exchange, and shared problem-solving	Semi-annually, or as approved by the COR
3.3 Coordination with Other Key Stakeholders	Guidance, tools, or other T/TA resources and strategies developed through convening proven experts, UCEDD representatives, and partners on emerging issues and priority topics	As developed and approved; summarize annually
3.4 Information Management System for PPR	Highly reliable, secure web-based information management system for electronic submission of Annual OIDD/UCEDD PPRs, including electronic storage of required documents, electronic transfer to OIDD, and data files to OIDD based on	Operational by contract start date or transition-

Submission	agency specifications	complete within 90 calendar days; continuous operation thereafter
3.4 Information Management System Change Accommodation	Change management/system enhancement approach that accommodates changes to information management systems as needed	Within 60 calendar days after contract start date; updated as needed
3.4 Information Management System Improvement	User testing, streamlined forms, enhanced guidance, reduced burden, improved impact capture, and tools to improve grantee use of their own data	Initial improvements by March 31 of the Base Year; updates thereafter as needed and approved
3.4 Information Management Training and Support	Training and technical assistance to UCEDD and federal staff on the web-based information management systems supported by this contract	Ongoing; monthly office hours and at least one annual comprehensive training
3.4 Information Management Reporting	Reports and data in accordance with OIDD format and guidelines	As requested; standard reports within 10 business days unless otherwise specified by OIDD/COR
3.4 Public-Facing Information Management System	Public-facing web-based information management system with functionality to categorically search past and current UCEDD initiatives, activities, and efforts	By September 30 of the Base Year; updated

		quarterly thereafter
4.1 Project Management and Evaluation	Annual summative evaluation report on extent to which T/TA has supported AT Programs in: 1. Implementing required state-level and leadership activities; 2. Achieving compliance with AT Act requirements; 3. Improving data collection quality and consistency; 4. Increasing AT access and acquisition; and Demonstrating program impact and outcomes	By September 30 of Base year and each Option Period
4.2(1)(a) Knowledge Development, Sharing, and Transfer	Develop, maintain, and redesign dynamic, state-of-the-art Website for AT Programs that is user-friendly, fully accessible, and 508 compliant	Initial launch by contract start date; ongoing maintenance monthly
4.2(2)(a-c) Knowledge Development, Sharing, and Transfer	High-quality trainings including: 1. Foundational training on AT Act; 2. Activity-specific training; 3. Data collection and reporting training;	Semi-annually as approved
4.2(3) Knowledge Development, Sharing, and Transfer	Rapid response and operational support to AT Programs and ACL staff	As requested
4.2(3) Knowledge Development, Sharing, and Transfer	Individualized, outcome-oriented T/TA to AT Programs for highly complex matters and circumstances	As requested
4.2(4) Knowledge Development, Sharing, and Transfer	Facilitate up to 2 training meetings annually with state and territory AT Program grantees regarding AT Act requirements, reporting requirements, reporting results, data system navigation, and other topics identified by ACL	Semi-annually or as scheduled with ACL
4.3(1) Collaboration	Electronic work plan(s) outlining shared goals/accountability with ACL for federal initiatives involving AT Programs	Work plans as required
4.4(1)(a) Information Management and Data Systems	Maintain and operate National Assistive Technology Data System (NATADS) or equivalent to remain operational for receipt of AT Annual Progress Reports	October 1 - December 31 annually; continuous system operation

4.4(1)(b) Information Management and Data Systems	Maintain and operate NATADS or equivalent for receipt of State Plans for Assistive Technology (3-year cycle)	August 1 - September 30 (60-day period) every 3 years; continuous system operation
4.4(1)(c) Information Management and Data Systems	Data export of the 56 state and territory AT Annual Progress Reports	AT APR by February 15 annually
4.4(1)(d) Information Management and Data Systems	Data export of the 56 state and territory AT State Plans	State Plans within 45 days of submission period close
4.4(2)(a) Information Management and Data Systems	Maintain CATADA Catalogue of Initiatives as repository of field-generated initiatives; review hundreds of state improvement outcomes and innovations submitted by AT Programs	Updated quarterly; comprehensive annual review by September 30

F.4 PAYMENT FOR UNAUTHORIZED WORK

No payments will be made for any unauthorized supplies and/or services or for any unauthorized changes to the work specified herein. This includes any services performed by the Contractor of their own volition or at the request of an individual other than a duly appointed Contracting Officer. Only a duly appointed Contracting Officer is authorized to change the specifications, terms, and conditions under this effort.

SECTION G - Contract Administration Data

G.1 PROVISIONS APPLICABLE TO DIRECT COSTS

Notwithstanding Clause 52.216-7 "Allowable Cost and Payment" and Clause 52.244-2 "Subcontracts", of the Federal Acquisition Regulation, unless otherwise expressly provided elsewhere in the contract or in any modification thereto, the cost of the following items or activities shall be unallowable as direct costs:

1. Acquisition by purchase or lease, of any interest in real property.
2. Special rearrangement or alteration of facilities;
3. Purchase or lease or rental of any item of general purpose; office furniture or office equipment (including data tapes);
4. Travel to foreign countries; and
5. Food and beverage costs unless part of per diem expenses paid in accordance with the Federal Travel Regulations.

Any equipment having a unit acquisition cost in excess of $1,000.00, of which the Contractor wishes to be reimbursed as a direct item of cost, shall not be acquired by the Contractor without the specific advance written approval of the Contracting Officer.

G.2 CONFERENCE EXPENSES

Unless the Contracting Officer provides explicit written approval for conference expenses, conference expenses are not allowable under this contract. For purposes of this contract, conference and conference expense are defined in the HHS Policy on Promoting Efficient Spending, specifically Attachment 1, Use of Appropriated Funds for Conferences and Meeting Space dated January 23, 2015. The attachment also provides a list of typical HHS meetings and events that are not considered conferences at Exhibit 2. The policy and associated attachments are located at the following site:
http://www.hhs.gov/grants/contracts/contract-policies-regulations/index.html)

G.3 GIFT CARD/CERTIFICATE EXPENSES

Unless the Contracting Officer provides explicit written approval for gift card/gift certificate expenses, such expenses are not allowable under this contract.

G.4 AUTHORITIES OF GOVERNMENT PERSONNEL

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

Contracting Officer

Christopher Poulos
Office of Acquisition Management Services
U.S. Department of Health and Human Services
5600 Fishers Lane
Rockville, MD 20857
Email: Christopher.Poulos@hhs.gov

Contracting Officer's Representative
Jack Brandt
Community Living Specialist,
Office of Intellectual and Developmental Disabilities
Jack.Brandt@acl.hhs.gov

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

G.5 CONTRACTING OFFICER'S REPRESENTATIVE (COR) AUTHORITY

(a) Performance of work under this contract must be subject to the technical direction of the Contracting Officer's Representative identified above, or a representative designated in writing. The term "technical direction" includes, without limitation, direction to the contractor that directs or redirects the labor effort, shifts the work between work areas or locations, fills in details and otherwise serves to ensure that tasks outlined in the work statement are accomplished satisfactorily.

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

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

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

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

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

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

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

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

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

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

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

G.6 INVOICES

Electronic Invoicing and Payment Requirements - Invoice Processing Platform (IPP)

- All Invoice submissions for goods and or services delivered to facilitate payments must be made electronically through the U.S. Department of Treasury's Invoice Processing Platform System (IPP).
- Invoice Submission for Payment means any request for contract financing payment or invoice payment by the Contractor. To constitute a proper invoice, the payment request must comply with the requirements identified in the applicable Prompt Payment clause included in the contract, or the clause 52.212-4 included in commercial items contracts. The IPP website address is: https://www.ipp.gov.
- The Agency will enroll the Contractors new to IPP. The Contractor must follow the IPP registration email instructions for enrollment to register the Collector Account for submitting invoice requests for payment. The Contractor Government Business Point of Contact (as listed in SAM) will receive Registration email from the Federal Reserve Bank of St. Louis (FRBSTL) within 3 – 5 business days of the contract award for new contracts or date of modification for existing contracts.
    - Registration emails are sent via email from ipp.noreply@mail.eroc.twai.gov. Contractor assistance with enrollment can be obtained by contacting the IPP Production Helpdesk via email to IPPCustomerSupport@fiscal.treasury.gov or phone (866) 973-3131.
    - The Contractor POC will receive two emails from **IPP Customer Support**, the first email contains the initial administrative IPP User ID. The second email, sent within 24 hours of receipt of the first email, contains a temporary password. You must log in with the temporary password within 30 days.
- If your company is already registered to use IPP, you will not be required to re-register.
- If the Contractor is unable to comply with the requirement to use IPP for submitting invoices for payment as authorized by HHSAR 332.7002, a written request must be submitted to the Contracting Officer to explain the circumstances that require the authorization of alternate payment procedures.

Additional Office of Acquisition Management Services (OAMS) requirements:

(i) The contractor shall submit invoices under this contract once per month. For indefinite delivery vehicles, separate invoices must be submitted for each order.

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

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

(iv) Invoices that include cost-reimbursement CLINs must be submitted in a format showing expenditures for that month, as well as contract cumulative amounts.
At a minimum the following cost information shall be included, in addition to supporting documentation to substantiate costs incurred.

- Direct Labor - include all persons, listing the person's name, title, number of hours worked, hourly rate, the total cost per person and a total amount for this category;
- Indirect Costs (i.e., Fringe Benefits, Overhead, General and Administrative, Other Indirects)- show rate, base and total amount;
- Consultants (if applicable) - include the name, number of days or hours worked, daily or hourly rate, and a total amount per consultant;
- Travel - include for each airplane or train trip taken the name of the traveler, date of travel, destination, the transportation costs including ground transportation shown separately and the per diem costs. Other travel costs shall also be listed;
- Subcontractors (if applicable) - include, for each subcontractor, the same data as required for the prime Contractor;
- Other Direct Costs - include a listing of all other direct charges to the contract, i.e., office supplies, telephone, duplication, postage; and
- Fee – amount as allowable in accordance with the Schedule and FAR 52.216-8 if applicable.

(v) Invoices submitted to IPP are limited to 10MB. Backup support should be sent to the contracting officer, contract specialist, and COR in the event it causes the file size to exceed the limit.

SECTION H - Special Contract Requirements

H.1 52.252-2 CLAUSES INCORPORATED BY REFERENCE. (FEB 1998)

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

H.2 PROHIBITION AGAINST PERSONAL SERVICES

The Contractor shall not perform personal services under this contract. Contractor personnel are employees of the Contractor or its subcontractors and are under the administrative control and supervision of the Contractor. A Contractor supervisor must give all individual Contractor employee assignments and daily work direction. The Government will not supervise or direct Contractor employees in the performance of their assignments. If at any time the Contractor believes that any Government action or communication has been given that would create a personal service relationship between the Government and any Contractor employee, the contractor shall promptly notify the Contracting Officer of this communication or action. The Contractor shall not perform any inherently-governmental functions under this contract. No Contractor employee shall represent or give the appearance that he/she is a Government employee, agent or representative. No Contractor employee shall state orally or in writing at any time that he or she is acting on behalf of the Government. The Contractor is responsible for ensuring that all employees assigned to this contract understand and are committed to following these requirements.

H.3 CONTRACTOR PERFORMANCE EVALUATION(S)

Contractor performance will be evaluated on an interim and final basis pursuant to FAR Subpart 42.15. Interim evaluations will occur on an annual basis upon the completion of the first year of the contract. The Contractor Performance Assessment Reporting System (CPARS) will be used for these reviews. Information on CPARS is located at http://www.cpars.gov.

Contractors may, at their discretion, use Attachment J.2 to submit a self-assessment to the COR and contracting officer to consider when documenting performance, at no additional cost. The self-assessment should be submitted to the COR and contracting officer at least 30 days prior to completion of the first year, and each following year.

H.4 POST AWARD ORGANIZATIONAL CONFLICT OF INTEREST

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

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

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

H.4 CONTRACTOR PERSONNEL IDENTIFICATION

Contractor and subcontractor employees are required to identify themselves as contractor personnel in all contract related meetings with government personnel, or the general public, and in all contract related communication, to include oral and written correspondence.

At a minimum, emails and voicemails shall include the following details:
Name, Functional Job Title
Contractor Company Name

On assignment with:
Applicable HHS Office
Other contact details as necessary

H.5 DEVIATED DEFINITIONS
The following revised FAR Part 2 definitions apply, when applicable, in accordance with HHS FAR Class Deviations 2025-01 and 2025-02.

2.101 Definitions.
* * * * *
Biobased product means a product determined by the U.S. Department of Agriculture to be a commercial product or industrial product (other than food or feed) that is composed, in whole or in significant part, of biological products, including renewable domestic agricultural materials and forestry materials, or that is an intermediate ingredient or feedstock. The term includes, with respect to forestry materials, forest products that meet biobased content requirements, notwithstanding the market share the product holds, the age of the product, or whether the market for the product is new or emerging. (7 U.S.C. 8101) (**7 CFR part 4270.2**).
* * * * *
Sustainable products and services means:

(1) Products containing recovered material designated by the U.S. Environmental Protection Agency (EPA) under the Comprehensive Procurement Guidelines (42 U.S.C. 6962) (40 CFR

part 247) (*https://www.epa.gov/smm/comprehensive-procurement-guideline-cpg-program#products*).
(2) Energy- and water-efficient products that are ENERGY STAR® certified or Federal Energy Management Program (FEMP)-designated products (42 U.S.C. 8259b) (10 CFR part 436, subpart C) (*https://www.energy.gov/eere/femp/search-energy-efficient-products and https://www.energystar.gov/products?s=mega*).
(3) Biobased products meeting the content requirement of the U.S. Department of Agriculture under the BioPreferred® program (7 U.S.C. 8102) (7 CFR part 3201[7 CFR part 4270]) (*https://www.biopreferred.gov*).
(4) Acceptable chemicals, products, and manufacturing processes listed under EPA's Significant New Alternatives Policy (SNAP) program, which ensures a safe and smooth transition away from substances that contribute to the depletion of stratospheric ozone (42 U.S.C. 7671l) (40 CFR part 82, subpart G) (*https://www.epa.gov/snap*).
* * * * *
United States, when used in a geographic sense, means the 50 States and the District of Columbia, except as follows: * * *

(9) Reserved
* * * * *

SECTION I - Contract Clauses

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

I.0 SPECIAL NOTICE

In accordance with HHS FAR Class Deviations 2025-01 and 2025-02 the following clauses do not apply to this order, unless a deviation is included herein:

- 52.222-9 Apprentices and Trainees
- 52.222-21 Prohibition of Segregated Facilities
- 52.222-26 Equal Opportunity
- 52.222-27 Affirmative Action Compliance Requirements for Construction
- 52.222-29, Notification of visa denial
- 52.223-2 Reporting of Biobased Products Under Service and Construction Contracts (MAY 2024)
- 52.223-10 Waste Reduction Program (MAY 2024)
- 52.223-19 Compliance with Environmental Management Systems
- 52.223-23 Sustainable Products and Services (MAY 2024)
- 52.244-6 Subcontracts for Commercial Products and Commercial Services (JAN 2025)

I.1 52.252-2 CLAUSES INCORPORATED BY REFERENCE. (FEB 1998)

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

FEDERAL ACQUISITION REGULATION (FAR) (48 CFR CHAPTER 1) CLAUSES

Clause No.	Title and Date
52.210-1	Market Research (Nov 2021)
52.203-2	Certificate of Independent Price Determination (April 1985)
52.203-13	Contractor Code of Business Ethics and Conduct (Nov 2021)
52.204-19	Incorporation by Reference of Representations and Certifications (Dec 2014)
52.222-43	Fair Labor Standards Act and Service Contract Act- Price Adjustment (Multiple Year and Option Contracts) (Aug 2018)
52.222-44	Fair labor Standards Act and Service Contract Act-Price Adjustment (May 2014)
52.22290	Addressing DEI Discrimination by Federal Contractors [Deviation, Pursuant to HHS Class Deviation 2026-01 Amendment 2 (Apr 2026)]
52.227-14	Rights in Data-General (May 2014)
52.232-1	Payments (April 1984)
52.232-8	Discounts for Prompt Payment (Feb 2002)
52.232-40	Providing Accelerated Payments to Small Business Subcontractors (Nov 2021)

52.244-2	Subcontracts (Jun 2020)

FEDERAL ACQUISITION REGULATION (FAR) (48 CFR CHAPTER 1) CLAUSES

FAR 52.204-19 Incorporation by Reference of Representations and Certifications (DEC 2014)

FAR 52.222-90 Addressing DEI Discrimination by Federal Contractors [Deviation, Pursuant to HHS Class Deviation 2026-01 Amendment 2 (Apr 2026)]

HEALTH AND HUMAN SERVICES ACQUISITION REGULATION (HHSAR) (48 CFR CHAPTER 3) CLAUSES

Clause No.	Title and Date
352.203-70	Anti-Lobbying (Dec 2015)
352.208-70	Printing and Duplication (Dec 2015)
352.211-3	Paperwork Reduction Act (Dec 2015)
352.222-70-	Contractor Cooperation in Equal Employment Opportunity Investigations (Dec 2015)
352.227-70	Publications and Publicity (Dec 2015)
352.231-70	Salary Rate Limitation (Dec 2015)
352.223-71	Instructions to Offerors - Sustainable Acquisition (Dec 2015)
352.232-71	Electronic Submission of Payment

352.204-71 INFORMATION AND INFORMATION SYSTEMS SECURITY (FEB 2024) (DEVIATION)

(a) Definitions. As used in this clause—
Breach means 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 personally identifiable information for an other than authorized purpose.

Business associate (see 45 CFR 160.103), except as provided in paragraph (2) of this definition, business associate means, with respect to a covered entity, a person who -

(1) On behalf of such covered entity or of an organized health care arrangement (as defined in this clause) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this contract or agreement, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or

(2) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in 45 CFR section 164.501), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(3) A covered entity may be a business associate of another covered entity.

(4) Business associate includes the following:

(i) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.

(ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity.

(iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

(5) Business associate does not include:

(i) A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.

(ii) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of 45 CFR 164.504(f) apply and are met.

(iii) A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law.

(iv) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement by virtue of such activities or services.

Business associate agreement means the agreement, or other arrangement, as dictated by the HIPAA Privacy Rule (45 CFR 160), between an HHS covered entity and a business associate, which must be entered into in addition to the underlying contract for services and before any disclosure (see 45 CFR 160.103) of PHI can be made to the business associate, in order for the business associate to perform certain functions or activities on behalf of an HHS entity.

Controlled unclassified information (CUI) means information that laws, regulations, or Government-wide policies require to have safeguarding or dissemination controls, excluding classified information.

Healthcare component means a component or combination of components of a hybrid entity designated by the hybrid entity in accordance with 45 CFR 164.105(a)(2)(iii)(D) (see 45 CFR 164.103). The Secretary of HHS has designated HHS as a covered entity (further designated as a "hybrid entity"), and has also designated four HHS divisions as healthcare components under HIPAA, including —

(1) The Centers for Medicare and Medicaid Services (CMS), insofar as it operates the fee-for-service Medicare program;

(2) The Program Support Center (PSC), Division of Commissioned Personnel, insofar as it operates a health plan for Commissioned Corps officers;

(3) The World Trade Center (WTC) Health Program; and,

(4) The Indian Health Service (IHS), insofar as it operates a health plan and a program providing healthcare that uses electronic transactions.

HHS Information Technology General Rules of Behavior means a set of HHS rules that describes the responsibilities and expected behavior of users of HHS information or information systems.

HHS sensitive information means all HHS data, on any storage media or in any form or format, which requires confidentiality, integrity, and availability protection due to the risk of harm that could result to interests of HHS, other agencies or entities, or individuals from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes—

(1) Information where the improper use or disclosure could adversely affect the ability of HHS to accomplish its mission, i.e., HHS proprietary information;

(2) Records about individuals requiring protection under laws and regulations such as the E-Government Act, Privacy Act and the HIPAA Privacy Rule, or based on a data use agreement or a promise or assurance of confidentiality; and

(3) Information that would be exempt from disclosure if requested under the Freedom of Information Act. Examples of HHS sensitive information include—

(i) Individually-identifiable medical, benefits, and personnel information;

(ii) Financial, budgetary, research, quality assurance, confidential commercial, critical infrastructure, security-sensitive, procurement-sensitive, investigatory, and law enforcement information;

(iii) Controlled unclassified information;

(iv) Information that would be confidential and privileged in litigation such as information protected by the deliberative process privilege, attorney work-product privilege, and the attorney-client privilege; and

(v) Other information which, if released, could result in a violation of law or agreement, could cause harm or unfairness to any individual or group, or could adversely affect the national interest or the conduct of Federal programs.

HIPAA Rules means the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and part 164.

Incident means an occurrence that (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information systems; or (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable policies.

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information system security plan means a formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements.

Information technology (see FAR 2.101) also means Information and Communication Technology (ICT).

Information technology-related contracts means those contracts that include services (including support services), and related resources for information technology.

Organized health care arrangement (see 45 CFR 160.103) means:

(1) A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;

(2) An organized system of health care in which more than one covered entity participates and in which the participating covered entities:

(i) Hold themselves out to the public as participating in a joint arrangement;

and

(ii) Participate in joint activities that include at least one of the following:

(A) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;

(B) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or

(C) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.

(3) A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan;

(4) A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or

(5) The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans.

Privacy officer means the HHS official(s) with responsibility for implementing and oversight of privacy related policies and practices that impact a given HHS acquisition.

(b) General. Contractors, subcontractors, their employees, third-parties, and business associates with access to HHS information, information systems, or information technology (IT) or providing and accessing IT-related goods and services, shall adhere to the HHS Cybersecurity Program and the directives and handbooks, complete HHS security training prior to accessing HHS information (including HHS sensitive information and information systems security and privacy) and on an annual basis thereafter, as well as those set forth in the contract specifications, statement of work, or performance work statement. These include, but are not limited to, HHS Personnel Security and Suitability Program, which establishes HHS procedures, responsibilities, and processes for complying with current Federal law, Executive Orders, policies, regulations, standards, and guidance for protecting HHS information, information systems (see 302.101, Definitions) security and privacy, and adhering to personnel security requirements when accessing HHS information or information systems.

(c) Access to HHS information and HHS information systems.

(1) Contractors are limited in their request for logical or physical access to HHS information or HHS information systems for their employees, subcontractors, third parties and business associates to the extent necessary to perform the services or provide the goods as specified in the contracts, agreements, task, delivery, or purchase orders.

(2) All Contractors, subcontractors, third parties, and business associates working with HHS information are subject to the same investigative requirements as those of HHS appointees or employees who have access to the same types of information. The level and process of background security investigations for Contractors to access HHS information and HHS

information systems shall be in accordance with HHS Personnel Security and Suitability Program.

(3) Contractors, subcontractors, third parties, and business associates who require access to national security programs must have a valid security clearance.

(4) 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.

(5) HIPAA business associate agreements. Under the HIPAA Privacy and Security Rules (see 45 CFR 164), pursuant to 45 CFR 164.502(e)(1), a covered entity may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain, or transmit protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor of a covered entity's business associate. Additionally, a business associate may disclose protected health information to a business associate that is a subcontractor and may allow the subcontractor to create, receive, maintain, or transmit protected health information on its behalf, if the business associate obtains satisfactory assurances, in accordance with 45 CFR 164.504(e)(1)(i), that the subcontractor will appropriately safeguard the information. The satisfactory assurances required by 45 CFR 45 CFR 164.504(e)(1) of this section shall be documented through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of 45 CFR 164.504(e). The contracts shall also include breach reporting policies and procedures for suspected or confirmed breaches of protected health information. The contract shall impose a duty to cooperate with the

healthcare component and/or HHS breach investigation and response and must require all subcontractors to comply with the same HIPAA Rules requirements as a condition of receiving government data.

(i) Contractors or entities required to execute business associate agreements for contracts and other agreements become HHS business associates. Business associate agreements are issued by HHS or may be issued by other HHS programs in support of HHS. The HIPAA Privacy Rule requires HHS to execute compliant business associate agreements with persons or entities that create, receive, maintain, or transmit HHS PHI or that will store, generate, access, exchange, process, or utilize such PHI in order to perform certain activities, functions or services to, for, or on behalf of HHS. There may be other HHS components or staff offices which also provide certain services and support to HHS and must receive PHI in order to do so. If these components award contracts or enter into other agreements, purchase/delivery orders, modifications and issue governmentwide purchase card transactions to help in the delivery of these services to HHS, they will also fall within the requirement to obtain a satisfactory assurance from these contractors by executing a business associate agreements.

(ii) Business associate agreement flow down to subcontractors. A prime contractor required to execute a business associate agreement shall also obtain a satisfactory assurance, in the form of a business associate agreement, of its subcontractors who will also create, receive, maintain, or transmit PHI or that will store, generate, access, exchange, process, or utilize such PHI will comply with HIPAA Rules requirements to the same degree as the Contractor. A contractor employing a subcontractor who creates, receives, maintains, or transmits PHI or that will store, generate, access, exchange, process, or utilize such PHI under a contract or agreement is required to execute a business associate agreement with each of its subcontractors which also obligates the subcontractor (i.e., also a business associate) to provide the same protections and safeguards and agree to the same disclosure restrictions to PHI that is required of the covered entity and the prime contractor.

(d) Contractor operations required to be in United States. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practicable. If such services are proposed to be performed outside the continental United States, and are not otherwise disallowed by other Federal law, regulations or policy, or other HHS policy or other mandates as stated in the contract, specifications, statement of work or performance work statement (including applicable business associate agreements), the Contractor/subcontractor must state in its proposal where all non-U.S. services are provided. At a minimum, the Contractor/subcontractor must include a detailed Information System Security Plan, for review and approval by the Contracting Officer, specifically to address mitigation of the resulting problems of communication, control, and data protection.

(e) Roster of employees. Contractors and subcontractors shall provide a roster containing the name, position, e-mail address, phone number, and responsibilities of each employee, including subcontractors, performing work under the contract to develop, have the ability to access, or host and/or maintain a government information system(s). The roster must be submitted to

Contracting Officer within **thirty (30) days** from the effective date of the contract. Revisions to the roster as a result of staffing changes must be submitted within the number of days of the change provided by the Contracting Officer. The Contracting Officer, or the Contracting Officer's Representative (COR), will notify the Contractor of the appropriate level of investigation required for each staff member based on the information provided on the roster. If an employee is filling a new position, the Contractor must provide a position description, and the Government will determine the appropriate suitability level.

(f) Contractor/subcontractor employee reassignment and termination notification. Contractors and subcontractors shall provide written notification to the Contracting Officer and COR immediately, and not later than four (4) hours, when an employee working on an HHS information system or with access to HHS information is reassigned or leaves the Contractor or subcontractor's employment on the cognizant HHS contract. The Contracting Officer and COR must also be notified immediately by the Contractor or subcontractor prior to an unfriendly termination.

(g) Non-disclosure agreement. The Contractor and subcontractors shall submit completed non-disclosure agreements, as provided by the Contracting Officer, for each employee having access to non-public government information under this contract. The non-disclosure agreements shall be submitted to the Contracting Officer prior to the performance of work.

(h) HHS information custodial requirements. (1) Release, publication, and use of data. Information made available to a Contractor or subcontractor by HHS for the performance or administration of a contract or information developed by the Contractor/subcontractor in performance or administration of a contract shall be used only for the stated contract purpose and shall not be used in any other way without HHS prior written approval. This clause expressly limits the Contractor's/subcontractor's rights to use data as described in 52.227-14, Rights in Data—General, paragraph (d).

(2) Media sanitization. HHS information shall not be co-mingled with any other data on the Contractors/subcontractor's information systems or media storage systems in order to ensure federal and HHS requirements related to data protection, information segregation, classification requirements, and media sanitization can be met (see HHS Cybersecurity Program). HHS reserves the right to conduct scheduled or unscheduled on- site inspections, assessments, or audits of Contractor and subcontractor IT resources, information systems and assets to ensure data security and privacy controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with Federal and HHS requirements. The Contractor and subcontractor will provide all necessary access and support to HHS and/or GAO staff during periodic control assessments or audits.

(3) Data retention, destruction and contractor self-certification. The Contactor and its subcontractors are responsible for collecting and destroying any HHS data provided, created, or stored under the terms of this contract, to a point where HHS data or materials are no longer readable or reconstructable to any degree, in accordance with NIST SP 800- 88, Guidelines for

Media Sanitization, or subsequent directive. Prior to termination or completion of this contract, the Contractor/subcontractor must provide its plan for destruction or return of all HHS data in its possession accordance with contract requirements or Contracting Officer instructions for disposition, including compliance with National Institute of Standards and Technology (NIST) SP 800-88, Guidelines for Media Sanitization, for the purposes of media sanitization on all IT equipment. The Contractor must certify in writing to the Contracting Officer within 30 days of termination of the contract that the data destruction requirements in this paragraph have been met.

(4) Return of HHS data and information. When information, data, documentary material, records and/or equipment is no longer required, it shall be returned to the HHS (as stipulated by the Contracting Officer or the COR) or the Contractor/subcontractor must hold it until otherwise directed. Items returned will be hand carried, securely mailed, emailed, or securely electronically transmitted to the Contracting Officer or to the address as provided in the contract or by the assigned COR, and/or accompanying business associate agreement. Depending on the method of return, Contractor/subcontractor must store, transport, or transmit HHS sensitive information, when permitted by the contract using HHS-approved encryption tools that are, at a minimum, validated under Federal Information Processing Standards (FIPS) 140-3 (or its successor). If mailed, Contractor/subcontractor must send via a trackable method (USPS, UPS, Federal Express, etc.) and immediately provide the Contracting Officer with the tracking information. No information, data, documentary material, records or equipment will be destroyed unless done in accordance with the terms of this contract and the HHS Agency Records Control Schedules (2019).

(5) Use of HHS data and information. The Contractor/subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of HHS information only in compliance with the terms of the contract and applicable Federal and HHS information confidentiality and security laws, regulations, and policies. If Federal or HHS information confidentiality and security laws, regulations, and policies become applicable to the HHS information or information systems after execution of the contract, or if the NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies for this contract as a result of any updates, if required.

(6) Copying HHS data or information. The Contractor/subcontractor shall not make copies of HHS information except as authorized and necessary to perform the terms of the contract or to preserve electronic information stored on Contractor/subcontractor electronic storage media for restoration in case any electronic equipment or data used by the Contractor/subcontractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.

(7) Violation of information custodial requirements. If HHS determines that the Contractor has violated any of HHS information confidentiality, privacy, or security provisions, it shall be sufficient grounds for HHS to withhold payment to the Contractor or third-party or terminate the

contract for default in accordance with FAR part 49 or terminate for cause in accordance with FAR 12.403.

(8) Encryption. The Contractor/subcontractor must store, transport, or transmit HHS sensitive information, when permitted by the contract, using cryptography, HHS encryption policies, and HHS-approved encryption tools that are, at a minimum, validated under FIPS 140-3 (or its successor).

(9) Firewall and web services security controls. The Contractor/subcontractor's firewall and Web services security controls, if applicable, shall meet or exceed HHS minimum requirements. HHS Configuration Standards Guidelines are available upon request.

(10) Disclosure of HHS data and information. Except for uses and disclosures of HHS information authorized in a cognizant contract for performance of the contract, the Contractor/subcontractor may use and disclose HHS information only in two other situations: (i) subject to paragraph 10 of this section, in response to a court order from a court of competent jurisdiction, or (ii) with HHS prior written approval. The Contractor/subcontractor must refer all requests for, demands for production of, or inquiries about, HHS information and information systems to the Contracting Officer for response. If the Contractor/subcontractor is in receipt of a court order or other request or believes it has a legal requirement to disclose HHS information, that Contractor/subcontractor shall immediately refer such court order or other request to the Contracting Officer for response. If the Contractor or subcontractor discloses information on behalf of HHS, the Contractor and/or subcontractor must maintain an accounting of disclosures. Accounting of Disclosures documentation maintained by the Contractor/subcontractor will include the name of the individual to whom the information pertains, the date of each disclosure, the nature or description of the information disclosed, a brief statement of the purpose of each disclosure or, in lieu of such statement, a copy of a written request for a disclosure, and the name and address of the person or agency to whom the disclosure was made. The Contractor/subcontractor will provide its Accounting of Disclosures upon request and within 15 calendar days to the assigned COR and Privacy Officer. Accounting of disclosures should be provided electronically via encrypted email to the COR and designated HHS facility Privacy Officer as provided in the contract, business associate agreement, or by the Contracting Officer. If providing the Accounting of disclosures electronically cannot be done securely, the Contractor/subcontractor will provide copies via trackable methods (UPS, USPS, Federal Express, etc.) immediately, providing the designated COR and Privacy Officer with the tracking information.

(11) Compliance with privacy statutes and applicable regulations. The Contractor/subcontractor shall not disclose HHS information protected by any of HHS privacy statutes or applicable regulations including, but not limited to, the Privacy Act of 1974 or the HIPAA Rules. If the Contractor/subcontractor is in receipt of a court order or other requests for HHS information or has questions if it can disclose information protected under the above-mentioned confidentiality statutes because it is required by law, that Contractor/subcontractor shall immediately refer such court order or other request to the Contracting Officer for response.

(i) Compliance with identification policies. Contractors shall comply with the 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; HHS Policy for Information Security and Privacy Protection (IS2P) Control Catalog, and Executive Order 13467, Part 1, section 1.2.

(j) Report of known or suspected incident or breach. The Contractor, subcontractor, third-party affiliate or business associate, and its employees shall notify HHS immediately via the Contracting Officer and the COR or within one (1) hour of a known or suspected incident or breach. The initial notification may first be made verbally but must be followed up in writing within one (1) hour. Report all actual or suspected incident and breach information to the Contracting Officer and the COR as identified in the contract or as directed in the contract, within one hour of discovery or suspicion.

(1) Such issues shall be remediated as quickly as is practical, but in no event longer than **30 days**. The Contractor shall notify the Contracting Officer in writing.

(2) When the security fixes involve installing third party patched (e.g., Microsoft OS patches or Adobe Acrobat), the Contractor will provide written notice to HHS that the patch has been validated as not affecting the systems within **1-3 days**. When the Contractor is responsible for operations or maintenance of the systems, they shall apply the security fixes within timeline required by HHS/OCIO policies and in accordance with supplemental requirements inserted in the contract.

(3) All other vulnerabilities shall be remediated in a timely manner based on risk, in accordance with the timelines specified in the HHS Policy for Vulnerability Management, and the HHS Standard for Plan of Action and Milestones (POAM) Management and Reporting. Contractors shall notify the Contracting Officer, and COR within 2 business days after remediation of the identified vulnerability. Exceptions to this paragraph (e.g., for the convenience of HHS) must be requested by the Contractor through the COR and shall only be granted with approval of the Contracting Officer and the Office of the Chief Information Officer (OCIO). These exceptions will be tracked by the Contractor in concert with the Government in accordance with HHS Policy for IT Procurements–Security and Privacy Language.

(k) Incident and breach investigation. (1) The Contractor/ subcontractor shall immediately notify the Contracting Officer and COR for the contract of any known or suspected incident or breach (see definitions, paragraph (a)), or any other unauthorized disclosure of sensitive information, including that contained in system(s) to which the Contractor/subcontractor has access.

(2) To the extent known by the Contractor/subcontractor, the Contractor/ subcontractor's notice to HHS shall identify the information involved, an estimate of the number of potentially impacted individuals, the circumstances surrounding the incident (including to whom, how, when, and where the HHS information or assets were placed at risk or compromised), and any other information that the Contractor/subcontractor considers relevant.

(3) With respect to unsecured protected health information, the business associate is deemed to have discovered an incident as defined above when the business associate either knew, or by exercising reasonable diligence should have been known to an employee of the business associate. Upon discovery, the business associate must notify HHS of the incident immediately within one hour of discovery or suspicion as agreed to in the business associate agreement.

(4) In instances of theft or break-in or other criminal activity, the Contractor/subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction. The Contractor, its employees, and its subcontractors and their employees shall cooperate with HHS and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The Contractor/subcontractor shall cooperate with HHS in any civil litigation to recover HHS information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

(l) Incident and breach notification requirements. (1) The Contractor/subcontractor shall provide notice to HHS of an incident as set forth in the incident and breach investigation section of this clause. The Contractor shall fully cooperate with HHS or third- party entity performing an independent risk analysis on behalf of HHS. Failure to cooperate may be deemed a material incident or breach and grounds for contract termination.

(2) The Contractor/subcontractor shall fully cooperate with the HHS Computer Security Incident Response Center (CSIRC), HHS Breach Response Team, Operating Divisions (OPDIVs), Staff Divisions (STAFFDIVs), other stakeholders or any Government agency conducting an analysis regarding any notice of an incident or breach, potential incident or breach, or incident which may require the Contractor to provide information to the Government or third-party performing a risk analysis for HHS, and shall address all relevant information concerning the incident or breach, including the following:

(i) Nature of the event (loss, theft, unauthorized access).

(ii) Description of the event, including:

(A) Date of occurrence.

(B) Date of incident or breach detection.

(C) Data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code.

(D) Number of individuals affected or potentially affected.

(E) Names of individuals or groups affected or potentially affected.

(F) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text.

(G) Amount of time the data has been out of HHS control.

(H) The likelihood that the sensitive information will or has been compromised (made accessible to and usable by unauthorized persons).

(I) Known misuses of data containing sensitive information, if any.

(J) Assessment of the potential harm to the affected individuals.

(K) Incident or breach analysis as outlined in the HHS Breach Response Policy and Plan, as appropriate.

(L) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive information that may have been compromised.

(M) Steps taken in response to mitigate or prevent a repetition of the

incident.

(m) Training. (1) All Contractor employees and subcontractor employees requiring access to HHS information or HHS information systems shall complete the following before being granted access to HHS information and its systems:

(i) On an annual basis, successfully complete the HHS Privacy and Information Security Awareness and HHS Information Security Rules of Behavior training.

(ii) On an annual basis, sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the HHS Information Security Rules of Behavior, relating to access to HHS information and information systems.

(iii) Successfully complete any additional cyber security or privacy training, as required for HHS personnel with equivalent information system access.

(2) The Contractor shall provide to the Contracting Officer and/or the COR a copy of the training certificates and affirmation that HHS Information Security Rules of Behavior signed by each applicable employee have been completed and submitted within five (5) days of the initiation of the contract and annually thereafter, as required.

(3) Failure to complete the mandatory annual training and acknowledgement of the HHS Information Security Rules of Behavior, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.

(n) Subcontract flow down. The Contractor shall include the substance of this clause, including this paragraph (k), in subcontracts, third-party agreements, and business associate agreements, of any amount and in which subcontractor employees, third-party servicers/employees, and business associates will perform functions where they will have access to HHS information (including HHS sensitive information), information systems, information technology (IT) or

providing and accessing information technology-related contract services, support services, and related resources (see HHSAR 302.101 definition of information technology-related contracts.)

(End of clause)

I.3.2 352.204-72 RECORDS MANAGEMENT (FEB 2024) (DEVIATION)

(a) Applicability. This clause applies to contracts that include Federal records, as defined in paragraph (b).

(b) Definition. As used in this clause—

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

(1) The term Federal record—

(i) Includes HHS records;

(ii) Does not include personal materials;

(iii) Applies to records created, received, or maintained by Contractors pursuant to their contract; and

(iv) May include deliverables and documentation associated with

deliverables.

(2) *Recorded information* means all traditional forms of records, regardless of physical form or characteristics, including information created, manipulated, communicated, or stored in digital or electronic form. (See 44 U.S.C. 3301.)

(3) *Personal materials* means documentary materials belonging to an individual that are not used to conduct agency business. Personal files are excluded from the definition of Federal records and are not owned by the Government. (See 36 CFR 1220.18.)

(c) Requirements.

(1) The Contractor shall comply with all applicable records management laws and regulations, as well as National Archives and Records Administration (NARA) records policies, including but not limited to the Federal Records Act (44 U.S.C. chapters 21, 29, 31, 33), NARA regulations at 36 CFR chapter XII subchapter B, and those policies associated with the safeguarding of records covered by the Privacy Act of 1974 (5 U.S.C. 552a). These policies include the preservation of all Federal records, regardless of form or characteristics, mode of transmission, or state of completion.

(2) In accordance with 36 CFR 1222.32, all data created for Government use and delivered to, or falling under the legal control of, the Government are Federal records subject to the provisions of 44 U.S.C. chapters 21, 29, 31, and 33, the Freedom of Information Act (FOIA) (5 U.S.C. 552), and the Privacy Act of 1974 (5 U.S.C. 552a), and must be managed and scheduled for disposition only as permitted by statute or regulation.

(3) In accordance with 36 CFR 1222.32, the Contractor shall maintain all Federal records created for Government use or created in the course of performing the contract and/or delivered to, or under the legal control of the Government and must be managed in accordance with Federal law. Electronic records and associated metadata must be accompanied by sufficient technical documentation to permit understanding and use of the records and data.

(4) The Contractor is responsible for preventing the alienation or unauthorized destruction of Federal records, including all forms of mutilation. Federal records may not be removed from the legal custody of HHS or destroyed except for in accordance with the provisions of the agency records schedules and with the written concurrence of the Contracting Officer. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. The Contractor shall report to the Contracting Officer any unlawful or accidental removal, defacing, alteration, or destruction of Federal records.

(5) The Contractor shall immediately notify the Contracting Officer upon discovery of any inadvertent or unauthorized disclosures of information, data, documentary materials, records or equipment. Disclosure of non-public information is limited to authorized personnel with a need-to-know as described in the contract. The Contractor shall ensure that appropriate personnel are trained to adhere to these contract requirements, and that applicable, administrative, technical, and physical safeguards are established to ensure the security and confidentiality of information, data, documentary material, Federal records and/or equipment is properly protected. The Contractor shall not remove Federal Records from Government facilities or systems, or facilities or systems operated or maintained on the Government's behalf, without the express written permission of the Contracting Officer. When information, data, documentary material, Federal records and/or equipment are no longer required, it shall be returned to HHS control or the Contractor must hold it until otherwise directed. Items returned to the Government shall be hand carried, mailed, emailed, or securely electronically transmitted to the Contracting Officer or as otherwise directed by the Contracting Officer. Destruction of Federal records is expressly prohibited unless in accordance with paragraph (c)(4).

(6) The Contractor shall only use Government information technology equipment for purposes specifically authorized by the contract and in accordance with HHS policy.

(7) The Contractor shall not create or maintain any Federal records containing any non-public HHS information that are not specifically authorized by the contract.

(8) The Contractor shall not retain, use, sell, or disseminate copies of any deliverable that contains information covered by the Privacy Act of 1974 or that which is generally protected from public disclosure by an exemption to the Freedom of Information Act.

(9) All Contractor employees assigned to this contract handle Federal records are required to take HHS-provided records management training. The Contractor is responsible for confirming training has been completed according to agency policies, including initial training and any annual or refresher training.

(d) Subcontract flowdown. The Contractor shall incorporate the substance of this clause, its terms and requirements including this paragraph, in all subcontracts under this contract.

(End of clause)

I.3.3 352.204-72 RECORDS MANAGEMENT (FEB 2024) (DEVIATION)

(a) Applicability. This clause applies to contracts that include Federal records, as defined in paragraph (b).

(b) Definition. As used in this clause—

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

(1) The term Federal record—

(i) Includes HHS records;

(ii) Does not include personal materials;

(iii) Applies to records created, received, or maintained by Contractors pursuant to their contract; and

(iv) May include deliverables and documentation associated with

deliverables.

(2) *Recorded information* means all traditional forms of records, regardless of physical form or characteristics, including information created, manipulated, communicated, or stored in digital or electronic form. (See 44 U.S.C. 3301.)

(3) *Personal materials* means documentary materials belonging to an individual that are not used to conduct agency business. Personal files are excluded from the definition of Federal records and are not owned by the Government. (See 36 CFR 1220.18.)

(c) Requirements.

(1) The Contractor shall comply with all applicable records management laws and regulations, as well as National Archives and Records Administration (NARA) records policies, including but not limited to the Federal Records Act (44 U.S.C. chapters 21, 29, 31, 33), NARA regulations at

36 CFR chapter XII subchapter B, and those policies associated with the safeguarding of records covered by the Privacy Act of 1974 (5 U.S.C. 552a). These policies include the preservation of all Federal records, regardless of form or characteristics, mode of transmission, or state of completion.

(2) In accordance with 36 CFR 1222.32, all data created for Government use and delivered to, or falling under the legal control of, the Government are Federal records subject to the provisions of 44 U.S.C. chapters 21, 29, 31, and 33, the Freedom of Information Act (FOIA) (5 U.S.C. 552), and the Privacy Act of 1974 (5 U.S.C. 552a), and must be managed and scheduled for disposition only as permitted by statute or regulation.

(3) In accordance with 36 CFR 1222.32, the Contractor shall maintain all Federal records created for Government use or created in the course of performing the contract and/or delivered to, or under the legal control of the Government and must be managed in accordance with Federal law. Electronic records and associated metadata must be accompanied by sufficient technical documentation to permit understanding and use of the records and data.

(4) The Contractor is responsible for preventing the alienation or unauthorized destruction of Federal records, including all forms of mutilation. Federal records may not be removed from the legal custody of HHS or destroyed except for in accordance with the provisions of the agency records schedules and with the written concurrence of the Contracting Officer. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. The Contractor shall report to the Contracting Officer any unlawful or accidental removal, defacing, alteration, or destruction of Federal records.

(5) The Contractor shall immediately notify the Contracting Officer upon discovery of any inadvertent or unauthorized disclosures of information, data, documentary materials, records or equipment. Disclosure of non-public information is limited to authorized personnel with a need-to-know as described in the contract. The Contractor shall ensure that appropriate personnel are trained to adhere to these contract requirements, and that applicable, administrative, technical, and physical safeguards are established to ensure the security and confidentiality of information, data, documentary material, Federal records and/or equipment is properly protected. The Contractor shall not remove Federal Records from Government facilities or systems, or facilities or systems operated or maintained on the Government's behalf, without the express written permission of the Contracting Officer. When information, data, documentary material, Federal records and/or equipment are no longer required, it shall be returned to HHS control or the Contractor must hold it until otherwise directed. Items returned to the Government shall be hand carried, mailed, emailed, or securely electronically transmitted to the Contracting Officer or as otherwise directed by the Contracting Officer. Destruction of Federal records is expressly prohibited unless in accordance with paragraph (c)(4).

(6) The Contractor shall only use Government information technology equipment for purposes specifically authorized by the contract and in accordance with HHS policy.

(7) The Contractor shall not create or maintain any Federal records containing any non-public HHS information that are not specifically authorized by the contract.

(8) The Contractor shall not retain, use, sell, or disseminate copies of any deliverable that contains information covered by the Privacy Act of 1974 or that which is generally protected from public disclosure by an exemption to the Freedom of Information Act.

(9) All Contractor employees assigned to this contract handle Federal records are required to take HHS-provided records management training. The Contractor is responsible for confirming training has been completed according to agency policies, including initial training and any annual or refresher training.

(d) Subcontract flowdown. The Contractor shall incorporate the substance of this clause, its terms and requirements including this paragraph, in all subcontracts under this contract.

(End of clause)

I.3.4 352.204-73 CONTRACTOR PERSONNEL SECURITY AND AGENCY ACCESS (FEB 2024) (DEVIATION)

(a) *Definitions.* As used in this clause—

Agency access means access to HHS facilities, sensitive information, information systems or other HHS resources.

Applicant means a contractor employee for whom the Contractor applies for an HHS identification card.

Contractor employee means a prime contractor and subcontractor employee who requires agency access to perform work under an HHS contract.

Identification card (or "ID card") means a government issued or accepted identification card such as a Personal Identity Verification (PIV) card, a PIV-Interoperable (PIV-I) card from an authorized PIV-1 issuer, or a non-PIV card issued by HHS, or a non-PIV card issued by another Federal agency and approved by HHS. PIV and PIV-1 cards have physical and electronic attributes that other (non-PIV) ID cards do not have.

Issuing office means the HHS entity that issues identification cards to contractor employees.

Local security servicing organization means the HHS entity that provides security services to the HHS organization sponsoring the contract.

(b) Risk and sensitivity level designations. For contracts requiring access to HHS facilities, sensitive information, information systems or other HHS resources, contractor employees will be required to complete background investigations, identity proofing, and government identification card application procedures to determine suitability for access.

HHS will assign a risk and sensitivity level designation to the overall contract and/or to contractor employee positions by category, group or individual. The risk and sensitivity level designations will be the basis for determining the level of personnel security processing required for contractor employees. The position sensitivity designation levels that apply will be identified in the contract. The following risk and sensitivity level designations and associated level of processing are required, and each level includes the prior levels—

(1) Low risk level: National Agency Check with Written Inquiries (NACI);
(2) Moderate risk level: Minimum Background Investigation (MBI); and
(3) High risk level: Background Investigation.

(c) Security clearances. Contractor employees may also be required to obtain security clearances (i.e., Confidential, Secret, or Top Secret). National Security work designated "special sensitive," "critical sensitive," or "non-critical sensitive," will determine the level of clearance required for contractor employees. Personnel security clearances for national security contracts in HHS will be processed according to the HHS Personnel Security and Suitability Program, HHS Instruction 731-1, and the Department of Defense National Industrial Security Program Operating Manual (NISPOM).

(d) Pre-screening of contractor employees. The Contractor must pre-screen individuals designated for employment under any HHS contract by verifying minimal suitability requirements to ensure that only candidates that appear to meet such requirements are considered for contract employment, and to mitigate the burden on the Government of conducting background investigations on objectionable applicants. The Contractor must exercise due diligence in pre-screening all employees prior to submission to HHS for agency access. HHS may decline to grant agency access to a contractor employee for reasons including, but not limited to—

(1) Conviction of a felony, a crime of violence, or a misdemeanor involving moral turpitude;

(2) Falsification of information entered on forms or of other documents submitted;

(3) Improper conduct including criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct or other conduct adverse to the Government regardless of whether the conduct is directly related to the contract; and

(4) Any behavior judged to pose a potential threat to HHS facilities, sensitive information, information systems or other resources.

(e) Citizenship status. The Contractor must monitor a non-citizen’s continued authorization for employment in the United States. The Contractor must provide documentation to the Contracting Officer or the Contracting Officer's Representative (COR) during the background investigation process that validates that the E-Verify requirement has been met for each contractor employee.

(f) Background investigation and adjudication. A contractor employee must have a favorable adjudication of background investigation before HHS will issue an ID card to the contractor employee granting access to HHS facilities, sensitive information, information systems or other HHS resources. HHS may accept favorable adjudications of background investigations from other Federal agencies when applicants have held PIV cards issued by those agencies with no break in service. HHS may also accept PIV-I (Interoperable) cards issued by an authorized PIV-1 issuer as evidence of identity. A favorable adjudication does not preclude HHS from initiating a new investigation when deemed necessary. At a minimum, the FBI National Criminal History Check (fingerprint check) must be favorably completed before an HHS identification card can be issued. Each Contractor must use the Office of Personnel Management's (OPM) e-QIP system, or successor system identified by HHS, to complete any required investigative forms. Instructions for obtaining fingerprints will be provided by the COR or Contracting Officer. The HHS Assistant Secretary for Administration, Program Support Center (PSC), or authorized HHS designee, is responsible for adjudicating the suitability of contractor employees.

(g) Agency access denied. Upon contract award, HHS will initiate the agency access procedure for all contractor employees requiring access to HHS facilities, sensitive information, controlled unclassified information, information systems, and other HHS resources for contract performance. HHS may deny agency access to any individual about whom an adverse suitability determination is made. Failure to submit the required security information or to truthfully answer all questions shall constitute grounds for denial of access. The Contractor must not provide agency access to contractor employees until the COR or Contracting Officer provides notice of approval, which is authorized only by the PSC, or authorized HHS designee. Where a proposed contractor employee is denied agency access by the Government or, if for any reason a proposed application is withdrawn by the Contractor during the agency access process, the additional costs and administrative burden for conducting additional background investigations caused by a lack of effective pre-screening or planning on the part of the Contractor may be considered as part of the Contractor's overall performance evaluation.

(h) Identification card application process. The COR will be the HHS ID card Sponsor and point of contact for the Contractor's application for an HHS ID card. The COR shall review and approve the HHS ID card application before an ID card is issued to the applicant. An applicant may be issued either a Personal Identity Verification (PIV) card that meets the standards of Homeland Presidential Security Directive (HSPD-12), or an applicant may be issued a non-PIV card. Generally, a non-PIV card will be issued for contracts that expire in six months or less, including option periods. The COR may request the issuing office to waive the six-month eligibility requirement when it is in HHS interest for contract performance. The following applies—

(1) PIV card. The applicant must complete an HHS on-line application for a PIV card;

(2) Non-PIV card. The applicant must complete and submit a hard copy of the

necessary form(s) to be provided to Contractor by COR/Sponsor) to the COR/Sponsor; and

(3) Regardless of the type of card to be issued (PIV or non-PIV), the applicant must appear in person to provide two forms of identity source documents in original form to HHS. The identity source documents must come from the list of acceptable documents included in Form F-9, OMB No. 1115-0136, Employment Eligibility Verification. At least one document must be a valid State or Federal government-issued picture identification. For a PIV card, the applicant may be required to appear in-person a second time for enrollment and activation.

(i) Identification card custody and control. The Contractor is responsible for the custody and control of all forms of government identification issued by HHS to contractor employees for access to HHS facilities, sensitive information, information systems and other HHS resources. The Contractor shall:

(1) Provide a listing of personnel for whom an identification (ID) card is requested to the COR who will provide a copy of the listing to the card issuing office. This may include Contractor and subcontractor personnel. Follow issuing office directions for submittal of an application package(s).

(2) While visiting or performing work on an HHS facility, as specified by the issuing office or COR, ensure that contractor employees prominently display their ID card.

(3) Immediately notify the COR or, if the COR is unavailable, the Contracting Officer when a contractor employee's status changes and no longer requires agency access (e.g., employee's transfer, completion of a project, retirement, removal from work on the contract, or termination of employment) that may affect the employee's eligibility for access to the facility, sensitive information, or resources.

(4) Promptly deliver to the issuing office: (a) all ID cards assigned to an employee who no longer requires access to the facility; and (b) all expired ID cards within five (5) days of their expiration or all cards at time of contract termination, whichever occurs first.

(5) Immediately report any lost or stolen ID cards to the issuing office and follow its instructions.

(i) The Contractor is responsible for maintaining and safeguarding the HHS ID card upon issuance to the contractor employee. The Contractor must ensure that contractor employees comply with HHS requirements concerning the renewal, loss, theft, or damage of an ID card. The Contractor must immediately notify the COR or, if the COR is unavailable, the Contracting Officer when an ID card is lost, stolen or damaged.

(ii) Failure to comply with the requirements for custody and control of HHS ID cards may result in withholding final payment or contract termination based on the potential for serious harm caused by inappropriate access to HHS facilities, sensitive information, information systems or other HHS resources.

(iii) Specific actions and activities are required in certain events—

(A) Renewal. A contractor employee's HHS issued ID card is valid for a maximum of three years or until the contract expiration date (including option periods), whichever occurs first. The renewal process should begin six weeks before the PIV card expiration date. If a PIV card is not renewed before it expires, the contractor employee will be required to sign-in daily for facility access and may have limited access to information systems and other resources.

(B) Lost/stolen. Immediately upon detection, the Contractor or contractor employee must report a lost or stolen HHS ID card to the COR, or if the COR is unavailable, the Contracting Officer, the issuing office, or the local servicing security organization. The Contractor must submit an incident report within 48 hours, through the COR or, if the COR is unavailable, the Contracting Officer, the issuing office, or the local security servicing organization describing the circumstances of the loss or theft. The Contractor must also report a lost or stolen PIV card through the HHS on-line registration system. If the loss or theft is reported by the Contractor to the local police, a copy of the police report must be provided to the COR or Contracting Officer. From the date of notification to HHS, the Contractor must wait three days before getting a replacement ID card. During the 3-day wait period, the contractor employee must sign in daily for facility access.

(C) Replacement. An ID card will be replaced if it is damaged, contains incorrect data, or is lost or stolen for more than 3 days, provided there is a continuing need for agency access to perform work under the contract.

(D) Surrender of ID cards. Upon notification that routine access to HHS facilities, sensitive information, information systems or other HHS resources is no longer required, the Contractor must surrender the HHS issued ID card to the COR, or if the COR is unavailable, the Contracting Officer, the issuing office, or the local security servicing organization in accordance with agency procedures.

(j) Flow down of clause. The Contractor is required to include this clause in any subcontracts at any tier that require the subcontractor or subcontractor's employees to have access to HHS facilities, sensitive information, information systems or other resources.

(End of clause)

I.3.5 352.224-70 NOTIFICATION OF SYSTEM OF RECORDS NOTICE (FEB 2024) (DEVIATION)

(a) This contract provides for the design, development, or operation of a system of records about individuals from which information about an individual is retrieved by the individual's name or by some other identifying particular assigned to the individual.

(b) The System of Records Notice(s) (SORN(s)) that is applicable to this contract is/are: see "Requirements for Procurements Involving Privacy Act Records" in Section C.

(c) The System of Records design, development, or operation work the Contractor is to perform is: see "Requirements for Procurements Involving Privacy Act Records" in Section C.

(d) The disposition to be made of the Privacy Act records upon completion of contract performance is as follows: see "Requirements for Procurements Involving Privacy Act Records" in Section C.

(e) Subcontract flow down. The Contractor is required to include this clause in all subcontracts at any tier performing work under the prime contract involving design, development, or operation work involving a System of Records.

(End of clause)

I.3.6 352.224-71 CONFIDENTIAL INFORMATION (FEB 2024) (DEVIATION)

(a) Definition. As used in this clause—

Confidential information means information or data of a personal nature about an individual, or proprietary information or data submitted by or pertaining to an institution or organization.

(b) Identification of information. Specific confidential information or categories of information that the Government will furnish to the Contractor, or that the Contractor is expected to generate, is identified in this contract.

(c) Disclosure. The Contractor shall not disclose confidential information or records written notice is provided to the Contracting Officer at least 45 days in advance of the Contractor's intent to release findings of studies or research, to which an agency response may be appropriate to protect the public interest or that of the agency. The Contractor shall not disseminate or publish such information without the written consent of the Contracting Officer.

(d) Government furnished or provided information: For information provided by or on behalf of the government—

(1) The publication or dissemination of the following types of information are restricted under this contract: **Non-public HHS APR program information, including Controlled Unclassified Information (CUI), procurement-sensitive information, privacy act-protected information (PII), internal deliberative materials, and confidential commercial information**.

(2) The reason(s) for restricting the types of information identified in subparagraph (d)(1) is/are: **Restrictions are necessary to protect non-public HHS APR reporting information and preserve the integrity of government operations. Unauthorized disclosure of CUI, procurement-sensitive information, internal deliberate materials, PII, or confidential commercial information could compromise acquisition processes, impair agency decision-making, violate privacy protections, or cause competitive harm to third parties**.

(e) The Contractor shall consult with the Contracting Officer when there is uncertainty with regard to the confidentiality of, or a property interest in, information under this contract prior to the release, disclosure, dissemination, or publication of such information.

(End of clause)

I.3.7 HHSAR 352.239-70 STANDARDS FOR HEALTH INFORMATION TECHNOLOGY (DEC 2022) (DEVIATION)

(a) *Definitions*. As used in this clause—

Health information technology (health IT) means hardware, software, integrated technologies or related licenses, intellectual property, upgrades, or packaged solutions sold as services that are designed for or support the use by health care entities or patients for the electronic creation, maintenance, access, or exchange of health information. (42 U.S.C. 300jj)
Individually identifiable health information means information that is a subset of health information, including demographic information collected from an individual, and:

(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

(i) That identifies the individual; or

(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual. (42 U.S.C. 300jj, 1320d)

ONC Health Information Technology Certification Program means the certification program administered by the HHS Office of the National Coordinator for Health Information Technology (ONC) using a third-party conformity assessment program for health IT. Certification criteria for the Program, which incorporate standards and implementation specifications in 45 CFR part 170 subpart B, are found in 45 CFR part 170, subpart C.

(b) Pursuant to the Health Information Technology for Economic and Clinical Health Act (HITECH Act), Pub. L. 111-5, Title XIII, sections 13111 and 13112, by submission of an offer and execution of a contract, the Contractor agrees that—

(1) For any work performed under the contract that involves implementing, acquiring, or upgrading health IT used for the direct exchange of individually identifiable health information between agencies and with non-Federal entities, the Contractor will utilize health IT that—

(i) Meets standards and implementation specifications adopted in 45 CFR part 170, subpart B, if such standards and implementation specifications can support the work performed under the contract; and

(ii) Is certified under the ONC Health Information Technology Certification Program, if certified technology can support the work performed under the contract (see certification criteria in 45 CFR part 170, subpart C), when the Contractor is an eligible professional in an ambulatory setting, or a hospital, eligible under sections 4101, 4102 and 4201 of the HITECH Act, or when the Contractor is implementing, acquiring or upgrading technology to be used by an eligible professional in an ambulatory setting, or a hospital, eligible under sections 4101, 4102 and 4201 of the HITECH Act.

(2) If the Contractor is a health care provider, health plan, or health insurance issuer, or is establishing an agreement with a health care provider, health plan, or health insurance issuer, for work performed under the contract that involves implementing, acquiring, or upgrading health IT, the Contractor will utilize health IT that—

(i) Meets standards and implementation specifications adopted in 45 CFR part 170, subpart B, if such standards and implementation specifications can support the work performed under the contract; and

(ii) Is certified under the ONC Health Information Technology Certification Program, if certified technology can support the work performed under the contract (see certification criteria in 45 CFR part 170, subpart C), when the Contractor is an eligible professional in an ambulatory setting, or a hospital, eligible under sections 4101, 4102 and 4201 of the HITECH Act, or when the Contractor is implementing, acquiring or upgrading technology to be used by an eligible professional in an ambulatory setting, or a hospital, eligible under sections 4101, 4102 and 4201 of the HITECH Act.

(c) If standards and implementation specifications adopted in 45 CFR part 170, subpart B, cannot support the work as specified in the contract, the Contractor is encouraged to use health IT that meets non-proprietary standards and implementation specifications developed by consensus-based standards development organizations. This may include standards identified in the ONC Interoperability Standards Advisory, available at https://www.healthit.gov/isa/.

(End of clause)

I.3.8 352.239-71 SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY RESOURCES (FEB 2024) (DEVIATION)

(a) Definitions. As used in this clause—

Information technology has the same meaning in FAR 2.101.

Information and communication technology (ICT) also means information technology (see FAR 2.101 for definitions).

Information system security plan means a formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements.

(b) Responsibilities. The Contractor shall be responsible for information technology security for all systems connected to a Department of Health and Human Services (HHS) network or operated by the Contractor for HHS, regardless of location. This clause is applicable to all or any part of the contract that includes information technology resources or services in which the Contractor has physical or other system access to HHS information that directly supports the mission of HHS. Examples of tasks that require security provisions include—

(1) Hosting of HHS e-Government sites or other information technology operations;

(2) Acquisition, transmission, or analysis of data owned by HHS with significant replacement cost should the contractor's copy be corrupted; and

(3) Access to HHS general support systems/major applications at a level beyond that granted the general public, e.g., bypassing a firewall.

(c) Information system security plan. The Contractor shall develop, provide, implement, and maintain an Information System Security Plan. HHS information system and platform information technology systems must have a security plan that provides an overview of the security requirements for the system and describes the security controls in place or the plan for meeting those requirements. Generally, this plan shall describe the processes and procedures that the Contractor will follow to ensure appropriate security of information system resources developed, processed, or used under this contract. The security plan should include implementation status, responsible entities, resources, and estimated completion dates. Security plans may also include, but are not limited to, a compiled list of system characteristics or qualities required for system registration, and key security-related documents such as a risk assessment, privacy impact assessment (PIA), system interconnection agreements, contingency plan, security configurations, configuration management plan, incident response plan, and the system privacy plan, as determined by the Contracting Officer’s Representative. The plan shall address the specific contract requirements regarding information systems or related support or services included in the contract, to include the PWS or SOW. The Contractor's Information System Security Plan shall comply with applicable Federal Laws that include, but are not limited to, 40 U.S.C. 11331, the Federal Information Security Modernization Act (FISMA) of 2014 and the E-Government Act of 2002. The plan shall meet information technology security requirements in accordance with Federal and HHS policies and procedures, and as amended during the term of this contract, and include, but are not limited to the following:

(1) OMB Circular A-130, Managing Information as a Strategic Resource;

(2) National Institute of Standards and Technology (NIST) Guidelines;

(3) Federal Information Processing Standard (FIPS) 200; and

(4) HHS Cybersecurity Program related to HHS information (including HHS sensitive information and information systems security and privacy), as well as those set forth in the contract specifications, statement of work, or performance work statement. These include, but are not limited to, the Cyber Security Checklist and Cyber Security Infographic at

https://www.hhs.gov/hipaa/for- professionals/security/guidance/cybersecurity/index.html, which provides HHS procedures, responsibilities, and processes for complying with current Federal law, Executive Orders, policies, regulations, standards and guidance for protecting HHS information, information systems (see 302.101, Definitions), information technology, and ICT, security and privacy, and adhering to personnel security requirements when accessing HHS information or information systems.

(d) Submittal of plan. Within 60 days after contract award, the Contractor shall submit the Information System Security Plan to the Contracting Officer for review and approval.

(e) Authority to Operate (ATO). As required by current HHS policy, the Contractor shall submit written proof of information technology security accreditation with a valid ATO to the Contracting Officer. Such written proof may be furnished either by the Contractor or by a third party. Accreditation shall be in accordance with HHS policy available from the Contracting Officer upon request. The Contractor shall submit for acceptance by the Contracting Officer along with this ATO a final security plan, risk assessment, security test and evaluation, privacy threshold analysis or privacy impact assessment, and a disaster recovery plan/continuity of operations plan.

(f) Annual validation. On an annual basis, the Contractor shall verify in writing to the Contracting Officer that the IT Security Plan remains valid.

(g) Banners. The Contractor shall ensure that the official HHS banners are displayed on all HHS systems (both public and private) operated by the Contractor that contain Privacy Act or other sensitive information before allowing anyone access to the system. The Office of Information Technology will make official HHS banners available to the Contractor.

(h) Screening and access. The Contractor shall screen all personnel requiring privileged access or limited privileged access to systems operated by the Contractor for HHS or interconnected to an HHS network in accordance with HHS policies referenced in paragraph (c).

(i) Training. The Contractor shall ensure that its employees performing services under this contract complete HHS security awareness and privacy training on an annual basis. This includes signing an acknowledgment on an annual basis that they have read, understand, and agree to abide by the HHS Rules of Behavior for the Use of HHS Information and IT Resources Policy as required; FAR 39.105, Privacy; clause 352.204-71, Information and Information Systems Security, and this clause.

(j) Government access. The Contractor shall provide the Government access to the Contractor's and subcontractors' facilities, installations, operations, documentation, information systems, databases, and personnel used in performance of the contract. The Contractor shall provide access to enable a program of information technology inspection (to include vulnerability testing), investigation and audit (to safeguard against threats and hazards to the integrity, availability and confidentiality of HHS data or to the function of information technology systems operated on behalf of HHS), and to preserve evidence of computer crime.

(k) Notification of termination of employees. The Contractor shall immediately notify the Contracting Officer when an employee who has access to HHS information systems or data terminates employment.

(l) Subcontract flow down requirement. The Contractor shall incorporate and flow down the substance of this clause to all subcontracts that meet the conditions in paragraph (a) of this clause.

(End of clause)

I.3.9 352.239-73 INFORMATION SYSTEM DESIGN AND DEVELOPMENT (FEB 2024) (DEVIATION)

(a) Design or development at non-HHS facilities. Information systems that are designed or developed for or on behalf of HHS at non-HHS facilities shall comply with all HHS directives developed in accordance with the Federal Information Security Modernization Act of 2014, Health Insurance Portability and Accountability Act (HIPAA) regulations, National Institute of Standards and Technology (NIST), and related HHS security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic protected health information (PHI), outlined in 45 CFR Part 164, Subpart C, information and system security categorization level designations in accordance with Federal Information Processing Standards (FIPS) 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199 system security categorization and the Trusted Internet Connections Reference Architecture.

(b) Privacy Impact Assessment. During the development cycle a Privacy Impact Assessment must be completed by the contractor, provided to the Contracting Officer Representative, and approved by the appropriate HHS and Operating Division security and privacy officials; government, contractor, or independent third party.

(c) Security of procured or developed systems and technologies. The Contractor shall ensure the security of all procured or developed systems and technologies, including their subcomponents (hereinafter referred to as "Systems"), throughout the life of the contract and any extension, warranty, or maintenance periods. This includes, but is not limited to, workarounds, patches, hotfixes, upgrades, and any physical components (hereafter referred to as Security Fixes) which may be necessary to fix all security vulnerabilities published or known to the Contractor anywhere in the Systems, including Operating Systems and firmware. The Contractor shall ensure that security fixes shall not negatively impact the Systems.

(d) Subcontract flow down requirements. The Contractor shall incorporate and flow down the substance of this clause to all subcontracts where services to perform information system design and development are required.

(End of clause)

I.3.10 352.239-74 INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE OR USE (FEB 2024) (DEVIATION)
(a) Definitions. As used in this clause—

Assessment and Authorization (A&A) means the process used to ensure information systems including Major Applications and General Support Systems have effective security safeguards which have been implemented, planned for, and documented in an Information Technology Security Plan. The A&A process per applicable HHS policies and procedures is the mechanism by which HHS provides an Authorization to Operate (ATO), the official management decision given by the HHS to authorize operation of an information system.

Information system security plan means a formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements.

(b) Hosting, operation, maintenance, or use at non-HHS facilities. For information systems that are hosted, operated, maintained, or used on behalf of HHS at non-HHS facilities, Contractors/subcontractors are fully responsible and accountable for ensuring compliance with all applicable Health Insurance Portability and Accountability (HIPAA) Act of 1996 (HIPAA) regulations, the Privacy Act and other required HHS confidentiality statutes included in HHS mandatory yearly training and privacy policy, Federal Information Security Modernization Act (FISMA), National Institutes of Standards and Technology (NIST), Federal Information Processing Standards (FIPS), and HHS security and privacy policy. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The Contractor's security and privacy control procedures must be equivalent to or exceed, those procedures used to secure HHS systems. A Privacy Impact Assessment (PIA) (if the system includes Personally Identifiable Information (PII)) or a Privacy Threshold Analysis (to determine if the system includes PII) must also be provided to the Contracting Officer Representative (COR) and approved by HHS Senior Agency Official for Privacy (SAOP) or designee prior to ATO. All external Internet connections to HHS network involving HHS information must be in accordance with the Trusted Internet Connections (TIC) Reference Architecture and reviewed and approved by HHS prior to implementation. For Cloud Services hosting, the Contractor shall also ensure compliance with the Federal Risk and Authorization Management Program (FedRAMP).

(c) Collecting, processing, transmitting, and storing of PII. Adequate security and privacy controls for collecting, processing, transmitting, and storing of PII, as determined by the HHS SAOP or designee, must be in place, tested, and approved by HHS prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of HHS. These security and privacy controls are to be assessed and stated within the PIA, Information System Security Plan, Information System Privacy Plan, Security Control Assessment Report, and/or Privacy Control Assessment Report, as agreed upon by the Contractor, COR, and the Operating Division Senior Official for Privacy. If these controls are determined not to be in place, or

inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection of PII.

(d) Annual FISMA security controls assessment. The Contractor/subcontractor's system must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the PIA. Any deficiencies noted during this assessment must be provided to the Contracting Officer for entry into HHS Plan of Action & Milestones (POA&M) management process. The Contractor/subcontractor must use HHS POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies must be corrected within the timeframes specified by the HHS in the performance work statement or statement of work, or in the approved remediation plan through the HHS POA&M process. Contractor/subcontractor procedures are subject to periodic, unannounced assessments by HHS officials, including the HHS Office of Inspector General. The physical security aspects associated with Contractor/subcontractor activities must also be subject to such assessments. The results of an annual review or a major change in the cybersecurity posture at any time may indicate the need for reassessment and reauthorization of the system. If major changes to the system occur that may affect the privacy or security of the data or the system, the A&A of the system may need to be reviewed, retested and re-authorized per HHS Rules of Behavior for the Use of HHS Information and IT Resources Policy. Major changes introducing new privacy risks require an updated and reapproved PIA.

(e) Annual self-assessment. The Contractor/subcontractor must conduct an annual self-assessment on all systems and outsourced services as required. Both hard copy and electronic copies of the assessment must be provided to the COR. HHS reserves the right to conduct such an assessment using government personnel or another Contractor/subcontractor. The Contractor/subcontractor must take appropriate and timely action, as may be specifically addressed in the contract, to correct or mitigate any weaknesses discovered during such testing, at no additional cost to the Government to correct Contractor/subcontractor systems and outsourced services.

(f) Prohibition of installation and use of personally-owned or Contractor-owned equipment or software on HHS networks. HHS prohibits the installation and use of personally-owned or Contractor/subcontractor-owned equipment or software on HHS networks. If non-HHS owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, performance work statement, statement of work, or contract. All of the security controls required for government furnished equipment must also be utilized in approved other equipment (OE) at the

Contractor’s expense. All remote systems must be equipped with, and use, an HHS- approved antivirus software and a personal (host-based or enclave based) firewall that is configured with an HHS-approved configuration. Software must be kept current, including all critical updates and patches. Owners of approved OE are responsible for providing and maintaining the anti-viral software and the firewall on the non-HHS owned OE.

(g) Disposal or return of electronic storage media on non-HHS leased or non-HHS owned IT equipment. All electronic storage media used on non-HHS leased or non-HHS owned IT equipment that is used to store, process, or access HHS information must be handled in adherence with disposition instructions upon—

(1) Completion or termination of the contract; or

(2) Disposal or return of the IT equipment by the Contractor/subcontractor or any person acting on behalf of the Contractor/subcontractor, whichever is earlier. Media (e.g., hard drives, optical disks, CDs, back-up tapes) used by the Contractors/ subcontractors that contain HHS information must be returned to the HHS for sanitization or destruction or the Contractor/subcontractor must self-certify that the media has been disposed of per disposition instructions. This must be completed within 30 days of termination of the contract.

(h) Bio-Medical devices and other equipment or systems. Bio-Medical devices and other equipment or systems containing media (e.g., hard drives, optical disks) with HHS sensitive information will not be returned to the Contractor at the end of lease, for trade-in, or other purposes. For purposes of these devices and protection of HHS sensitive information the devices may be provided back to the Contractor under one of three scenarios—

(1) The Contractor must accept the system without the drive;

(2) A spare drive must be installed in place of the original drive at time of turn- in if HHS initial medical device purchase included a spare drive; or

(3) The Contractor may request reimbursement for the drive at a reasonable open market replacement cost to be separately negotiated by the Contracting Officer and the Contractor at time of contract closeout.

(End of clause)

I.3.11 352.239-75 SECURITY CONTROLS COMPLIANCE TESTING (FEB 2024) (DEVIATION)

On a periodic basis, HHS, including the Office of Inspector General, reserves the right to evaluate any or all of the security controls and privacy controls implemented by the Contractor under the clauses contained within the contract. With 10 working-days' notice, at the request of the government, the Contractor must fully cooperate and assist in a government-sponsored security controls assessment at each location wherein HHS information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of HHS, including those initiated by the Office of Inspector General. The government may conduct a security control assessment on shorter notice, to include unannounced assessments, as determined by HHS in the event of an incident or a breach, or at any other time.

(End of clause)

I.3.12 352.239-76 SECURITY REQUIREMENTS FOR GOVERNMENT-OWNED CONTRACTOR-OPERATED AND CONTRACTOR-OWNED CONTRACTOR- OPERATED RESOURCES (FEB 2024) (DEVIATION)

(a) Federal policies. The Contractor shall comply with applicable federal laws, regulations, and HHS policies that include, but are not limited to—

(1) HHS Policy for Information Security and Privacy Protection (IS2P);

(2) Federal Information Security Modernization Act (FISMA) of 2014, (44 U.S.C. 101);

(3) National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, latest revision, Security and Privacy Controls for Information Systems and Organizations;

(4) Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource; and

(5) Any other applicable federal laws, regulations, NIST guidance, and local HHS

policies.

(b) Assessment and Authorization (A&A). A valid authority to operate (ATO) certifies that the Contractor's information system meets the contract's requirements to protect the agency data. If the system under this contract does not have a valid ATO, the Contractor shall work with the agency and supply the deliverables required to complete the ATO within the specified timeline(s) of **One Year.** The Contractor must conduct the A&A requirements in accordance with HHS IS2P, NIST SP 800-37, Guide for Applying the Risk Management Framework to Information Systems: A Security Life Cycle Approach (latest revision), NIST SP 800-53B, Control Baselines for Information Systems and Organizations, and the NIST SP 800-53A (latest revision). HHS acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the system security and privacy controls are implemented and operating effectively.

(1) A&A package deliverables. The Contractor shall provide an A&A package within **9 months** to the Contracting Officer and/or the Contracting Officer's Representative (COR). The following A&A deliverables are required to complete the A&A package—

(i) Accessibility Reports and ACL Systems Technical Specifications

(ii) A System Security Plan (SSP) is due: **Digital submission to SecureIT@acl.hhs.gov or approved repository by 9 months.** The SSP shall comply with the NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems, the Federal Information Processing Standard (FIPS) 200, Recommended Security Controls for Information Systems, and NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations applicable baseline requirements, and other applicable NIST guidance as well as HHS policies and other guidance. The SSP must be consistent with and detail the approach to IT security contained in the Contractor's bid or proposal that resulted in the award of this contract. The SSP must provide an overview of the system environment and security requirements to protect the

information system (see HHSAR 302.101, Definitions) as well as describe all applicable security controls in place or planned for meeting those requirements. It should provide a structured process for planning adequate, cost-effective security protection for a system. The Contractor shall review and update the SSP at least annually thereafter and if requested, provide a copy of the updated SSP to the COR.

(iii) A Security Assessment Plan/Report (SAP/SAR) is due: **Digital submission to SecureIT@acl.hhs.gov or approved repository by 6 months** The security assessment must be conducted by **Independent third-party assessment for security vulnerabilities and privacy impact or vendor assessment for security vulnerabilities and privacy impact assessment** and be consistent with NIST SP 800-53A, NIST SP 800-30, and HHS policies. The assessor will document the assessment results in the SAR. Thereafter, the Contractor, in coordination with the COR shall conduct, or as directed, in the assessment of the security controls **3 months from package receipt** and update the SAR at least annually. A copy of the updated SAR shall be provided to the COR, if requested.

(iv) All systems shall have a completed privacy threshold analysis (PTA). If the PTA results determines the system contains personally identifiable information, a privacy impact assessment, approved by the HHS SAOP, is required.

(v) System Privacy Plan and Privacy Control Assessment. As required in OMB Circular A-130, a System Privacy Plan and Privacy Control Assessment shall be included in A&A. The plan and assessment may be included in the Security System Plan, or a separate report in the A&A, as determined by the COR.

(vi) An Independent Assessment is due **within 6 months**. The Contractor shall have an independent third-party validate the security and privacy controls in place for the system(s) commensurate with the risk levels per NIST SP 800-53B. The independent third party shall review and analyze the security authorization package and report on technical, operational, and management level deficiencies as outlined in NIST SP 800-53. The Contractor shall address all "high" deficiencies before submitting the package to the Government for acceptance and document all remaining deficiencies in a system Plan of Actions and Milestones (POA&M).

(vii) The POA&M is due as follows—

(A) **1-2 days** from the date the weaknesses are formally identified and documented;

(B) Critical-risk weaknesses must be mitigated within **15 days** from the date the weaknesses are formally identified and documented;

(C) High-risk weaknesses must be mitigated **30 calendar days** from the date the weaknesses are formally identified and documented;

(D) Medium weaknesses must be mitigated within **60 calendar days** from the date the weaknesses are formally identified and documented; and

(E) Low weaknesses must be mitigated within **180 calendar days** from the date the weaknesses are formally identified and documented.

(2) HHS will determine the risk rating of all vulnerabilities. Identified risks stemming from deficiencies related to the security control baseline implementation, assessment, continuous monitoring, vulnerability scanning, flaws and security defect in a system (that require to create a patch for remediation), and other security reviews and sources, as documented in the SAR, shall be documented and tracked by the Contractor for mitigation in the POA&M document consistent with the HHS Standard for Plan of Action and Milestones policies. Depending on the severity of the risks, HHS may require designated POA&M weaknesses to be remediated before an ATO is issued. Thereafter, continue to remediate weaknesses throughout the contract. The POA&M document shall be updated at least quarterly and **Monthly via meeting, email to SecureIT@acl.hhs.gov and/or approved repository with notification**.

(3) A Contingency Plan and Contingency Plan Test are due: **Plans need to be submitted with the A&A package and execution of the tested yearly at a minimum once yearly from date of authorization**. The Contingency Plan shall be developed in accordance with NIST SP 800-34, Contingency Planning Guide for Federal Information Systems, and be consistent with HHS policies. Upon final acceptance by the System Owner, the Contractor, in coordination with the COR and System Owner, shall test the Contingency Plan and prepare a Contingency Plan Test Report that includes the test results, lessons learned, and any remaining action items to be addressed. The Contractor shall update and test the Contingency Plan at least annually.

(4) An E-Authentication Questionnaire is required. The Contractor shall collaborate with at the COR's direction to ensure that the E-Authentication Guidance requirements are implemented in accordance with OMB 04-04 and NIST SP 800-63 series, latest versions. Based on the level of assurance determined by the E-Authentication, the Contractor shall ensure appropriate authentication to the system, including remote authentication, is in-place in accordance with the assurance level determined by the E- Authentication (when required), in accordance with HHS Guidance for Selection of e- Authentication Assurance Levels and any other applicable HHS policies.

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

(6) Annual assessment/penetration (pen) test. The Contractor shall assess the system security and privacy controls (or ensure an assessment of the controls is conducted) at least annually to determine the implemented security and privacy controls are operating as intended and producing the desired results (this involves penetration testing conducted by the agency or independent third-party and **Weekly DHS Cyber Hygiene scans, monthly vulnerability scans,**

adhoc vulnerability scans, pre and post deployment vulnerability scans, adhoc SynAck continuous security and vulnerability disclosure testing, and monthly accessibility reviews. In addition, review all relevant A&A documentation (SSP, POA&M, Contingency Plan, etc.) and provide updates by the specified due date provided by the COR.

(7) Asset management. Using any available Security Content Automation Protocol (SCAP)-compliant automated tools for active/passive scans, the Contractor shall provide an inventory of all information technology (IT) assets for hardware and software (computers, servers, routers, databases, operating systems, etc.) that are processing HHS- owned information and/or data. It is anticipated that this inventory information will be required to be produced at least **Monthly**. IT asset inventory information shall include—

(i) IP address;

(ii) Machine name;

(iii) Operating system level;

(iv) Security patch level; and

(v) SCAP-compliant format information. The Contractor shall maintain a capability to provide an inventory of 100% of its IT assets using SCAP-compliant automated tools in accordance with the HHS Policy for Information Technology Asset Management (ITAM) and any other applicable HHS policy.

(8) Configuration management. The Contractor shall use available SCAP- compliant automated tools as per NIST IR 7511 and HHS Minimum Security Configurations Standards Guidance to scan all IT assets, including but not limited to computers, servers, routers, databases, operating systems, application, etc., that store and process government information. The Contractor shall provide scan reports to the COR upon request. The Contractor shall maintain a capability to provide security configuration compliance information for 100% of its IT assets using SCAP-compliant automated tools.

(9) Vulnerability management. The Contractor shall actively manage system vulnerabilities using automated tools and technologies where practicable and in accordance with HHS Policy for Vulnerability Management. Automated tools must be compliant with NIST-specified SCAP standards for vulnerability identification and management. The contractor shall maintain a capability to provide security vulnerability scanning information for 100% of IT assets using SCAP-compliant automated tools and report to the agency at least **Monthly with weekly check-**ins.

(10) Patching and vulnerability remediation. The Contractor shall install vendor- released security patches and remediate critical and high vulnerabilities in systems processing government information in an expedited manner, within vendor and agency specified timeframes.

(11) Secure coding. The Contractor shall follow the HHS Policy for Software Development Secure Coding Practices and secure coding best practice requirements, as directed by United States Computer Emergency Readiness Team specified standards, the Software Engineering Institute (SEI) CERT and the Open Web Application Security Project, that will limit system software vulnerability exploits.

(12) Boundary protection. The Contractor shall ensure that government information, other than unrestricted information, being transmitted from federal government entities to external entities is routed through a Trusted Internet Connection.

(13) Government access for security assessment.

(i) In addition to the Inspection Clause in the contract, the Contractor 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. This access includes, but is not limited to—

(1) 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, access to 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. For the purposes of this paragraph only, Government includes, but is not limited to, Contracting Officer, COR, the U.S. Department of Justice, U.S. Government Accountability Office, and the HHS Office of the Inspector General (OIG). The purpose of 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, Structured Query Language injection vulnerabilities, and any other known vulnerabilities.

(2) 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.

(ii) The Contractor shall segregate Government protected information and metadata on the handling of Government protected information from other information. Commingling of information is prohibited. Government inspectors, auditors, and investigators will not be precluded from having access to the sought information if sought information is commingled with other information.

(iii) The Contractor shall cooperate with inspections, audits, investigations,

and reviews.

(c) End of Life compliance. The Contractor shall 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 if it impacts enterprise-wide systems and services, or by the OPDIV CISO if it impacts only the OPDIV). The contractor must retire and/or upgrade all software/systems that have reached end-of-life in accordance with HHS End of Life Operating Systems, Software and Application Policy.

(d) Desktops, laptops, and other computing devices required for use by the Contractor. The Contractor 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:

(1) Encrypt equipment and sensitive information stored and/or processed by such equipment in accordance with HHS encryption standard and current FIPS 140 validation certificate from the NIST Cryptographic Module Validation Program.

(2) Configure laptops and desktops in accordance with the latest applicable United States Government Configuration Baseline, **DISA STIGs** and HHS Minimum Security Configuration Standards;

(3) Maintain the latest operating system patch release and anti-virus software definitions at least **Monthly scheduled time frame and adhoc for any emerging exploits according to risk assessed timeline**;

(4) 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

(5) Automate configuration settings and configuration management in accordance with HHS security policies, including but not limited to:

(i) Configuring its systems to allow for periodic HHS vulnerability and security configuration assessment scanning; and

(ii) Using SCAP-validated tools with capabilities to scan its systems at least on a monthly basis and report the results of these scans to the Contracting Officer and/or COR, Project Officer, and any other point of contract designated by the Contracting Officer or COR.

(e) Rights to data. Contractors shall specify any data rights asserted and mark such deliverables accordingly in accordance with applicable data rights clauses set forth in the contract.

(f) Information and Communications Technology (ICT) Cybersecurity Supply Chain Risk Management (C-SCRM) requirements. The Contractor shall secure their ICT supply chain in compliance with HHS Policy for Cyber Supply Chain Risk Management and Public Law 115-232, section 889. At a minimum, the Contractor shall—

(1) Develop rules for suppliers' development methods, techniques, or practices;

(2) Use secondary market components;

(3) Prohibit counterfeit products;

(4) Dispose and/or retain elements such as components, data, or intellectual property securely;

(5) Ensure adequate supply of components;

(6) 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;

(7) 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;

(8) Establish Service Level Agreements (SLAs), patching vehicles, and disclosure requirements in the case of an incident or new vulnerability being discovered; and

(9) 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

(10) Prohibit the use of covered telecommunications and video surveillance equipment or services.

(g) Subcontract flow down. The Contractor shall include the substance of this clause, including this paragraph (g), in subcontracts and third-party agreements, at any tier, of any amount and in which subcontractor employees and third-party servicers/employees, will perform functions or provide products under the scope of this contract, and have access to HHS information (including HHS sensitive information, i.e., protected health information), information systems, information technology (IT) or providing and accessing information technology-related contract services, support services, and related resources (see HHSAR 302.101, Definitions).

(End of clause)

I.3.13 352.239-77 CLOUD COMPUTING SERVICES (FEB 2024) (DEVIATION)

(a) Responsibilities. This clause is applicable to all or any part of the contract that includes cloud computing services. The Contractor shall be responsible for the following privacy and security requirements on this contract—

(1) Federal Risk and Authorization Management Program (FedRAMP) compliant authorization to operate. Compliance with FedRAMP Assessment and Authorization (A&A) requirements and ensure the information system/service (see HHSAR 302.101, Definitions) under this contract has an approved FedRAMP compliant authority to operate (ATO) in accordance with Federal Information Processing Standard (FIPS) Publication 199 defined security categorization. If a FedRAMP compliant ATO has not been granted, the Contractor must submit a plan to obtain a FedRAMP compliant ATO within **1Year**.

(i) Implement applicable FedRAMP baseline controls commensurate with the agency-defined security categorization and the applicable FedRAMP security control baseline available at fedramp.gov). The HHS Policy for Information Security and Privacy Protection (IS2P) and HHS Cloud Computing and Federal Risk and Authorization Management Program (FedRAMP) Guidance further define the baseline policies as well as roles and responsibilities. The Contractor shall implement additional controls identified by the agency in this contract.

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

(2) Data jurisdiction. The Contractor shall store all information within the security authorization boundary, data at rest, or data backup, within the Continental United States, and **No other locations outside the Continental United States**.

(3) Service Level Agreements (SLAs). When applicable, the Contractor shall understand the terms of the service agreements that define the legal relationships between cloud customers and the cloud service provider and work with the Contracting Officer's Representative (COR) to develop and maintain an SLA, as provided in the contract.

(4) Interconnection Agreements/Memorandum of Agreements. When applicable and identified in this contract, the Contractor shall establish and maintain interconnection agreements and or memorandum of agreements/understanding in accordance with HHS policies.

(b) Protection of information in a cloud environment.

(1) If Contractor personnel shall remove any information from the primary work area, they shall protect it to the same extent they would the proprietary data and/or company trade secrets and in accordance with HHS policies, available at https://www.hhs.gov/web/governance/digital-strategy/it-policy-archive/index.html.

(2) HHS will retain unrestricted rights to federal data handled under this contract. Specifically, HHS retains ownership of any user created/loaded data and applications collected, maintained, used, or operated on behalf of HHS and hosted on Contractor's infrastructure, as well as maintains the right to request full copies of these at any time. If requested, data shall be made available to HHS, at no additional cost, within one (1) business day from the date of the request, or within the timeframe otherwise specified.

(3) The Contractor shall ensure that the facilities that house the network infrastructure are physically and logically secure in accordance with FedRAMP requirements and HHS policies.

(4) The Contractor shall comply with NARA-approved records schedule(s) and protection requirements for federal agency electronic records in accordance with 36 CFR 1236.20 and 1236.22 (ref. a), including but not limited to —

(i) Maintenance of links between records and metadata; and

(ii) Categorization of records to manage retention and disposal, either through transfer of permanent records to NARA or deletion of temporary records in accordance with NARA-approved retention schedules.

(5) The disposition of all HHS data shall be at the written direction of the COR. This may include documents returned to HHS control, destroyed, or held as specified until otherwise directed. Items returned to the Government shall be hand carried or sent by certified mail to the COR.

(i) If the system involves the design, development, or operation of a system of records on individuals, the Contractor shall comply with the Privacy Act requirements in accordance with HHSAR 352.224-70, FAR 52.224-1 and 52.224-2.

(c) Assessment and Authorization (A&A) process.

(1) The Contractor shall comply with HHS and FedRAMP requirements as mandated by federal laws, regulations, privacy policies, and HHS policies, including making available any documentation, physical access, and logical access needed to support the A&A requirement. The level of effort for the A&A is based on the system's FIPS 199 security categorization and HHS security policies.

Certification must be completed in **3 months.**

(i) In addition to the FedRAMP compliant ATO, the Contractor shall complete and maintain an agency A&A package to obtain agency ATO prior to system deployment/service implementation. **Accessibility reports to be included by the time A&A package is submitted for review**. The agency ATO must be approved by the HHS authorizing official (AO) prior to implementation of system and/or service being acquired.

(ii) Cloud Service Provider (CSP) systems categorized as FIPS 199 High, Moderate or Low are recommended but not required to leverage a FedRAMP accredited Third Party Assessment Organization (3PAO). A CSP's agency partner may choose to use their own Independent Verification and Validation (IV&V) organization or 3PAO to assess the system. If an agency chooses to use their own IV&V team or an unaccredited 3PAO, they must submit an attestation regarding the team's independence to the agency and the FedRAMP PMO, and the IV&V / 3PAO team must use FedRAMP templates for the assessment and follow all FedRAMP requirements.

(iii) For all cloud services, the A&A package must contain the following documentation:

Completed ACL SSP Template for inherited security controls and defined agency controls, PTA/PIA, SAP and SAR, and POA&Ms.

(iv) Following the initial ATO, the Contractor shall review and maintain the ATO in accordance with HHS policies. The following templates and timelines are applicable.

(2) HHS reserves the right to perform penetration testing on all systems operated on behalf of the agency. If the Contracting Officer exercises this right, the Contractor shall allow HHS employees (and/or designated third parties) to conduct Security Assessment activities to include control reviews in accordance with HHS requirements. Review activities include, but are not limited to—

(i) Scanning operating systems, web applications, wireless scanning;

(ii) Network device scanning to include routers, switches, and firewall, and

IDS/IPS; and,

(iii) Databases and other applicable systems, including general support structure, that support the processing, transportation, storage, or security of Government information for vulnerabilities.

(3) The Contractor shall identify any gaps between required FedRAMP Security Control Baseline/Continuous Monitoring controls and the Contractor's implementation status as documented in the Security Assessment Report and related Continuous Monitoring artifacts. In addition, the Contractor shall document and track all gaps for mitigation in a Plan of Action and Milestones (POA&M) document. Depending on the severity of the risks, HHS may require remediation at the Contractor's expense before HHS issues an ATO.

(4) The Contractor shall mitigate security risks for which they are responsible, including those identified during A&A and continuous monitoring activities. All vulnerabilities and findings shall be remediated in accordance with timelines specified in the HHS POA&M Standard from discovery—

(i) Critical vulnerabilities no later than fifteen (15) days;

(ii) High within thirty (30) days;

(iii) Medium within ninety (90) days; and

(iv) Low vulnerabilities no later than three hundred and sixty (360) days, unless otherwise specified.

(v) In the event a vulnerability or other risk finding cannot be mitigated within the prescribed timelines above, they must be added to the designated POA&M and mitigated within the newly designated timelines: **Critical 15 days, High 30 days, Med 90 days, low 180 days. ACL time frame for Med is 60 days**. HHS will determine the risk rating of vulnerabilities using FedRAMP baselines.

(5) Revocation of a cloud service. HHS has the right to take action in response to the CSP's lack of compliance and/or increased level of risk. In the event the CSP fails to meet HHS and FedRAMP security and privacy requirements and/or there is an incident involving sensitive information (see HHSAR 302.101, Definitions), HHS may suspend or revoke an existing agency ATO (either in part or in whole) and/or cease operations. If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the CSP to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor information system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the internet, other networks, or applying additional security controls.

(d) Reporting and continuous monitoring.

(1) Following the initial ATOs, the Contractor shall perform the minimum ongoing continuous monitoring activities, submit required deliverables by the specified due dates, and meet with the system/service owner and other relevant stakeholders to discuss the ongoing continuous monitoring activities, findings, and other relevant matters. The CSP will work with the agency to schedule ongoing continuous monitoring activities. The minimum ongoing continuous monitoring activities include—

Monthly communication via meeting, email to SecureIT, and/or defined repository.

(2) At a minimum, the Contractor shall provide the following artifacts/deliverables on a monthly basis—

Email to SecureIT@acl.hhs.tov and/or designated repository if applicable:

(i) Operating system, database, Web application, and network vulnerability scan results;

(ii) Updated POA&Ms;

(iii) Any updated authorization package documentation as required by the annual attestation/assessment/review or as requested by the System Owner or AO, and;

(iv) Any configuration changes to the system and/or system components or CSP's cloud environment, that may impact HHS security posture. Changes to the configuration of the system,

its components, or environment that may impact the security posture of the system under this contract shall be approved by the agency.

(e) Configuration baseline.

(1) The Contractor shall certify that applications are fully functional and operate correctly as intended on systems using HHS Minimum Security Configurations Standards Guidance. The standard installation, operation, maintenance, updates, and/or patching of software must not alter the configuration settings from the approved HHS configuration baseline, **unless authorized by ACL for agency specific configurations**.

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

(f) Report of known or suspected incident or breach. The Contractor, subcontractor, third-party affiliate or business associate, and its employees shall notify HHS immediately via the Contracting Officer and the COR or within one (1) hour of an known or suspected incident or breach. The initial notification may first be made verbally but must be followed up in writing within one (1) hour. Report all actual or suspected incident and breach information to the Contracting Officer and the COR as identified in the contract or as directed in the contract, within one hour of discovery or suspicion.

(1) Such issues shall be remediated as quickly as is practical, but in no event longer than **15 days**. The Contractor shall notify the Contracting Officer in writing.

(2) When the security fixes involve installing third party patched (e.g., Microsoft OS patches or Adobe Acrobat), the Contractor will provide written notice to HHS that the patch has been validated as not affecting the systems within 10 working days. When the Contractor is responsible for operations or maintenance of the systems, they shall apply the security fixes within **30 days**.

(3) All other vulnerabilities shall be remediated in a timely manner based on risk, in accordance with the timelines specified in the HHS Policy for Vulnerability Management, and the HHS Standard for Plan of Action and Milestones (POAM) Management and Reporting. Contractors shall notify the Contracting Officer, and COR within 2 business days after remediation of the identified vulnerability. Exceptions to this paragraph (e.g., for the convenience of HHS) must be requested by the Contractor through the COR and shall only be granted with approval of the Contracting Officer and the Office of the Chief Information Officer (OCIO). These exceptions will be tracked by the Contractor in concert with the Government in accordance with HHS Policy for IT Procurements–- Security and Privacy Language.

(g) Incident and breach investigation. (1) The Contractor/ subcontractor shall immediately notify the Contracting Officer and COR for the contract of any known or suspected incident or breach (see definitions, paragraph (a)), or any other unauthorized disclosure of sensitive information, including that contained in system(s) to which the Contractor/subcontractor has access.

(2) To the extent known by the Contractor/subcontractor, the Contractor/ subcontractor's notice to HHS shall identify the information involved, an estimate of the number of potentially impacted individuals, the circumstances surrounding the incident (including to whom, how, when, and where the HHS information or assets were placed at risk or compromised), and any other information that the Contractor/subcontractor considers relevant.

(3) With respect to unsecured protected health information, the business associate is deemed to have discovered an incident as defined above when the business associate either knew, or by exercising reasonable diligence should have been known to an employee of the business associate. Upon discovery, the business associate must notify HHS of the incident immediately within one hour of discovery or suspicion as agreed to in the business associate agreement.

(4) In instances of theft or break-in or other criminal activity, the Contractor/subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction. The Contractor, its employees, and its subcontractors and their employees shall cooperate with HHS and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The Contractor/subcontractor shall cooperate with HHS in any civil litigation to recover HHS information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

(h) Incident and breach notification requirements. (1) The Contractor/subcontractor shall provide notice to HHS of a privacy or incident as set forth in the incident and breach investigation section of this clause. The Contractor shall fully cooperate with HHS or third- party entity performing an independent risk analysis on behalf of HHS. Failure to cooperate may be deemed a material incident or breach and grounds for contract termination.

(2) The Contractor/subcontractor shall fully cooperate with the HHS Computer Security Incident Response Center (CSIRC), HHS Breach Response Team, Operating Divisions (OPDIVs), Staff Divisions (STAFFDIVs), other stakeholders or any Government agency conducting an analysis regarding any notice of an incident or breach, potential incident or breach, or incident which may require the Contractor to provide information to the Government or third-party performing a risk analysis for HHS, and shall address all relevant information concerning the incident or breach, including the following:

(i) Nature of the event (loss, theft, unauthorized access).

(ii) Description of the event, including:

(A) Date of occurrence.

(B) Date of incident or breach detection.

(C) Data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code.

(D) Number of individuals affected or potentially affected.

(E) Names of individuals or groups affected or potentially affected.

(F) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text.

(G) Amount of time the data has been out of HHS control.

(H) The likelihood that the sensitive information will or has been compromised (made accessible to and usable by unauthorized persons).

(I) Known misuses of data containing sensitive information, if any.

(J) Assessment of the potential harm to the affected individuals.

(K) Incident or breach analysis as outlined in the HHS Breach Response Policy and Plan, as appropriate.

(L) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive information that may have been compromised.

(M) Steps taken in response to mitigate or prevent a repetition of the

incident.

(i) Media transport.

(1) The Contractor shall be accountable and document all activities associated with the transport of government information, devices, and media transported outside controlled areas and/or facilities. These include information stored on digital and non- digital media (e.g., CD-ROM, tapes, etc.), mobile/portable devices (e.g., USB flash drives, external hard drives, and SD cards).

Minimum requirements are: **Encrypted**.

(2) All information, devices and media shall be encrypted with HHS-approved encryption mechanisms to protect the confidentiality, integrity, and availability of all government information transported outside of controlled facilities.

(j) Boundary Protection—Trusted Internet Connections (TIC).

(1) The Contractor shall ensure that government information (other than unrestricted information) being transmitted from Federal government entities to external entities using cloud services is inspected by TIC processes that are in compliance with the requirements of the Office of Management and Budget Memorandum 19-26: Update to the TIC Initiative, TIC 3.0.

(2) The Contractor shall route all external connections through a TIC.

(3) Non-Repudiation. The Contractor shall provide a system that implements encryption with current FIPS 140 validation certificate from the NIST Cryptographic Module Validation Program that provides for origin authentication, data integrity, and signer non-repudiation.

(k) Subcontract flow down. The Contractor shall include the substance of this clause, including this paragraph (i), in subcontracts and third-party agreements, of any amount and in which subcontractor employees, and third-party servicers/employees, will perform functions where they will provide cloud computing services and have access to HHS information (including HHS sensitive information, i.e., protected health information (see HHSAR 302.101, Definitions)), information systems, information technology (IT) or providing and accessing information technology-related contract services, support services, and related resources (see HHSAR 302.101 definition of information technology-related contracts).

(End of clause)

352.239-79 INFORMATION AND COMMUNICATION TECHNOLOGY ACCESSIBILITY (FEB 2024) (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 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 may be identified in the specification, statement of work, or performance work statement. 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.

(End of clause)

I.4 FAR CLAUSES IN FULL TEXT

I.2.1 FAR 52.252-6 AUTHORIZED DEVIATIONS IN CLAUSES (NOV 2020)

(a) The use in this solicitation or contract of any Federal Acquisition Regulation (48 CFR Chapter 1) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the date of the clause.

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

(End of clause)

I.4.2 FAR 52.217-8 OPTION TO EXTEND SERVICES (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor prior to the expiration date of the contract.

I.4.3 FAR 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

- The Government may extend the term of this contract by written notice to the Contractor within 30 days of expiration of the contract provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 30 days before the contract expires. The preliminary notice does not commit the Government to an extension.

- If the Government exercises this option, the extended contract shall be considered to include this option clause.
- The total duration of this contract, including the exercise of any options under this clause, shall not exceed 6 years.

(a) The Government may extend the term of this contract by written notice to the Contractor at any time prior to contract expiration; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 6 years.

I.5 HHSAR 352.232-71 Electronic Submission of Payment Requests (FEB 2022)

(a) *Definitions.* As used in this clause—

Payment request means a bill, voucher, invoice, or request for contract financing payment with associated supporting documentation. The payment request must comply with the requirements identified in FAR 32.905(b), “Content of Invoices” and the applicable Payment clause included in this contract.

(b) Except as provided in paragraph (c) of this clause, the Contractor shall submit payment requests electronically using the Department of Treasury Invoice Processing Platform (IPP) or successor system. Information regarding IPP, including IPP Customer Support contact information, is available at *www.ipp.gov* or any successor site.
(c) The Contractor may submit payment requests using other than IPP only when the Contracting Officer authorizes alternate procedures in writing in accordance with HHS procedures.
(d) If alternate payment procedures are authorized, the Contractor shall include a copy of the Contracting Officer's written authorization with each payment request.

SECTION J – List of Attachments

Reference Number	Title	Number of Pages
J.1	Certificate of Current Cost of Pricing Data	1
J.2	Self-Assessment Template	4
J.3	Past Performance Questionnaire	7

SECTION K - Representations, Certifications, and Other Statements of Offerors or Respondents

K.0 SPECIAL NOTICE

System updates may lag policy updates. The System for Award Management (SAM) may continue to require entities to complete representations based on provisions that are not included in agency solicitations. Examples include 52.222-25, Affirmative Action Compliance, 52.223-22, Public Disclosure of Greenhouse Gas Emissions and Reduction Goals—Representation, and paragraphs (d) and (t) of 52.212-3, Offeror Representations and Certifications—Commercial Products and Commercial Services. Contracting officers will not consider these representations when making award decisions or enforce requirements. Entities are not required to, nor are they able to, update their entity registration to remove these representations in SAM.

The Contracting Officer will rely on the representations and certifications made by the schedule contractor at the contract level, deviated as follows.

(End of provision)

The following provisions do not apply to this order in accordance with HHS FAR Class Deviations 2025-01 and 2025-02:

52.222-22 Previous Contracts and Compliance Reports
52.222-23 Notice of Requirement for Affirmative Action to Ensure Equal Employment Opportunity for Construction.
52.222-24 Preaward On-Site Equal Opportunity Compliance Evaluation
52.222-25 Affirmative Action Compliance
52.223-22, Public Disclosure of Greenhouse Gas Emissions and Reduction Goals—Representation

SECTION L - Instructions, Conditions, and Notices to Offerors or Respondents

L.0 52.252-1 SOLICITATION PROVISIONS INCORPORATED BY REFERENCE. (FEB 1998)

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

FEDERAL ACQUISITION REGULATION (FAR) (48 CFR CHAPTER 1) PROVISIONS

Reserved

HEALTH AND HUMAN SERVICES ACQUISITION REGULATION (HHSAR) (48 CFR CHAPTER 3) PROVISIONS

Clause No.	Title and Date
352.239-73	Electronic and Information Technology Accessibility (Dec 2015)

L.1 FAR PROVISIONS IN FULL TEXT

FAR 52.252-5 AUTHORIZED DEVIATIONS IN PROVISIONS (NOV 2020

(a) The use in this solicitation of any Federal Acquisition Regulation (48 CFR Chapter 1) provision with an authorized deviation is indicated by the addition of "(DEVIATION)" after the date of the provision.

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

(End of provision)

L.2 HHSAR PROVISIONS IN FULL TEXT

L.2.1 HHSAR 352.239-78 Information and Communication Technology Accessibility Notice (FEB 2024) (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. 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. 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.

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 HHS Section 508 Evaluation Template are available at https://Section508.gov/.

In order to facilitate the Government's determination whether proposed ICT services meet applicable Section 508 accessibility standards, 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.

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.

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.

L.3 52.216-1 TYPE OF CONTRACT. (APR 1984)

The Government contemplates award of a Cost Plus Fixed Fee contract resulting from this solicitation.

(End of provision)

L.3.1 52.233-2 SERVICE OF PROTEST. (SEP 2006)

(a) Protests, as defined in section 33.101 of the Federal Acquisition Regulation, that are filed directly with an agency, and copies of any protests that are filed with the Government Accountability Office (GAO), shall be served on the Contracting Officer (addressed as follows) by obtaining written and dated acknowledgment of receipt from the Contracting Officer at the email address specified in Section G of the solicitation.

(b) The copy of any protest shall be received in the office designated above within one day of filing a protest with the GAO.

(End of provision)

L.3.2 FAR 52.252-5 AUTHORIZED DEVIATIONS IN PROVISIONS (NOV 2020)

(a) The use in this solicitation of any Federal Acquisition Regulation (48 CFR Chapter 1) provision with an authorized deviation is indicated by the addition of "(DEVIATION)" after the date of the provision.

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

(End of provision)

L.4 INQUIRIES/SUBMISSION

All questions/inquiries concerning the solicitation document must be submitted by e-mail (no faxes or telephone calls please) to the Contract Specialist, no later than **July 16, 2026, at 3:00 pm Eastern Time**. Questions should be e-mailed to the following address: Christopher.Poulos@hhs.gov. The Government's response to the inquiries will be email to SAM.Gov. Any resulting additions, deletions or changes to the solicitation will be made by issuance of a formal amendment. Quoters are instructed specifically to contact only the issuing contract office in connection with any aspect of this requirement prior to contract award. The

Government does not intend to extend the due date for quotes.

The quote must be submitted no later than **July 30, 2026, at 3:00 pm Eastern Time**. Late quotes will not be accepted. The Quoter shall submit their quote by email to the following address: Christopher.Poulos@hhs.gov.

L.8 GENERAL INSTRUCTIONS

The following instructions establish the acceptable minimum requirements for the format and content of your proposal. The Contracting Officer is the only individual authorized to legally commit the Government to the expenditure of public funds in connection with this requirement. By submitting a proposal in response to this solicitation, it is understood that your proposal shall become a part of the official contract file.

Your attention is directed to the requirements for the submission of technical proposals, and business proposals contained in Sections L.9, L.10 and L.11, of the solicitation. Your proposal must be submitted in accordance with these instructions.

Any resultant contract shall include the Federal Acquisition Regulation clauses applicable to the Offeror's organization and the type of contract awarded. The text of these clauses may be obtained at http://www.acquisition.gov/far/. Any additional clauses required by public law, executive order, or acquisition regulations, in effect at the time of the execution of the proposed contract, will be included.

The proposal must be prepared in three parts: a "Technical Proposal", a "Business Proposal" and a "Past Performance Information Volume. Each of these parts shall be separate and complete in itself so that the evaluation of one may be accomplished independently of the evaluation of the others.

L.9 TECHNICAL PROPOSAL INSTRUCTIONS

Technical proposals shall be limited to 20 double-spaced pages, with 1-inch margins, and using not less than 12 point font. Offerors are encouraged to be succinct and economical in their presentation. Excessive volume and elaborate presentation are unnecessary. Tables of contents and works cited and the Technical Appendices are not included in the page count.

The technical proposal must not contain references to cost; however, resource information, such as data concerning labor hours and categories, materials, subcontracts, etc., must be contained in the technical proposal so that your understanding of the scope of work may be evaluated. It must disclose your technical approach in sufficient detail to provide a clear and concise presentation that includes, but is not limited to, the requirements of the technical proposal instructions. The proposal shall contain a response to each of the factors and subfactors identified in Section L and will be evaluated in accordance with Section M. Proposals which merely offer to conduct a project in accordance with the requirements of the Government's scope of work will not be eligible for award. The technical proposal should reflect a clear understanding of the nature of

the work being undertaken.

Technical Appendices:
The technical appendices shall only include transcripts, resumes, and letters of commitment.

The technical proposal shall address the following factors:

L.9.1 FACTOR 1 - Technical Acceptability (Acceptable/Unacceptable)

L.9.2 SUBFACTOR 1 - Integrated Technical Approach (Acceptable/Unacceptable)

L.9.3 SUBFACTOR 2 - Information Management, Data Systems, and Website Operations (Acceptable/Unacceptable)

L.9.4 SUBFACTOR 3 - Management and Staffing (Acceptable/Unacceptable)

L.9.5 SUBFACTOR 4 - Accessibility, Security, and Privacy (Acceptable/Unacceptable)

L.9.6 FACTOR 2 – Price

L.9.7 FACTOR 3 – Information and Communication Technology Accessibility (Acceptable/Unacceptable)

Quoters shall provide the information and documentation required by HHSAR 352.239-78.

Quoters must explain how the development/creation efforts associated with the objectives will be measured to achieve HHS digital accessibility conformance standards and meet the legal framework of Section 508 standards. For each proposed ICT supply, license, product, or platform, and documentation a fully completed Accessibility Conformance Report (ACR) must be submitted. An ACR can be built from the Voluntary Product Accessibility Template (VPAT) or applicable HHS conformance checklist(s).

For ICT services, the quoter must provide information on how the services conform to Section 508 applicability standards.

Quoters must identify any inability to conform to Section 508 requirements and potential exceptions and exemptions in FAR subparts 39.204 and 39.205.

HHSAR 352.239-78 Information and Communication Technology Accessibility Notice (FEB 2024) (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. 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. 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.

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 HHS Section 508 Evaluation Template are available at https://Section508.gov/.

In order to facilitate the Government's determination whether proposed ICT services meet applicable Section 508 accessibility standards, 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.

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.

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.

(End provision)

L.10 BUSINESS PROPOSAL INSTRUCTIONS (Cost Reimbursement)

The Business Proposal shall contain the following information:

L.10.1 Offerors must complete and include Standard Form 33, blocks 12 through 18. Completion of this form indicates that the Offeror agrees with all the terms and conditions contained in solicitation Sections A through M. In addition, the proposal must contain a statement to the effect that it is firm for a period of at least 120 days from the date of receipt thereof by the Government.

L.10.2 Offerors shall include a completed copy of Section B of the solicitation in its proposal. Business proposals shall present cost estimates for each contract line item (CLIN) specified in Section B as well as the cumulative cost estimate for the entire contract.

L.10.4 Cost or Pricing Data

(a) Submission of certified cost or pricing data is not required.
(b) Provide the data described below:

The Offeror shall submit a cost proposal, with numbered pages, indexed, and fully supported by the information requested below, adequate to determine the reasonableness of costs proposed, to evaluate whether the proposed costs are consistent with the technical proposal and level of effort anticipated, and/or evaluate cost realism. The cost proposal shall describe the cost-element breakdown consistent with the Offeror's cost accounting system, and include a narrative to clearly describe in detail all supporting explanations of, or rationale for, all proposed costs. Cost elements 1 through 6 shall be addressed by each task per CLIN.

1. Direct Labor - Direct labor cost estimates shall be supported with breakdowns by individual tasks including the number of labor hours estimated for each proposed specific individual and/or labor category and their corresponding proposed hourly labor rate. The Offeror must submit source-type supporting documentation for all proposed labor rates in the form of excerpts from recent payroll registers or paystubs, salary surveys, similar positions from active similar contracts or task orders, salary rate schedules, written offers of employment, employment agreements or contracts that clearly indicate the position, annual salary and hourly rate for each position (include mapping if necessary). The proposal shall indicate whether current rates or escalated rates are used. If an escalation rate is incorporated, state the percent and methodology, e.g., fixed escalation factor applied to a base rate as of a specified date, or proposed escalated rate for the period of performance. The proposal shall include plans for any additional compensation resulting from salary increases in accordance with established company policy.

2. Other Direct Costs - Include in this category estimated costs for all other direct costs associated with providing the type of service to be acquired (e.g., consultant, subcontracts, transportation/ travel, supplies and equipment, communications, etc.). A complete explanation

of each element of cost, detailing the rationale used in developing the estimate must be included as well as source-type supporting documentation for each ODC proposed (e.g., previous invoice/bill from vendor, consultant/subcontractor agreement, catalog, published price list, available online/website cost information, etc.).

3. Indirect Costs - Indirect costs shall be proposed in accordance with the Offeror's current negotiated indirect cost rate agreement. The Offeror shall provide the name, address and telephone number of its cognizant Government audit agency and a copy of its current negotiated indirect cost rate agreement. If the Offeror does not have a ~~ne~~gotiated indirect cost rate agreement, the offeror must submit a schedule of indirect cost expenditures based upon their most recently completed accounting period (or management projections if offeror has been an entity for less than a year). The schedule must show in complete detail all of the cost elements that comprise each indirect cost pool (e.g. fringe benefits, overhead, G&A, etc.) along with the base and the calculation for the rate. Further, the offeror shall provide their detailed financial statements in order to verify the calculations and figures shown in schedule. The offeror's proposed indirect cost rates must be fully justified and are subject to negotiation.

4. Fee - The Offeror shall propose a fixed fee appropriate to their type of organization and in accordance with the statutory limitations specified in the FAR.

5. Facilities/Equipment - It is HHS policy that Contractors shall provide all facilities and equipment necessary for performance of contracts. Exceptions may be granted to furnish Government-owned property, only when approved by the head of the procuring activity. If additional equipment must be acquired, the Offeror shall include the description, estimated cost and source-type supporting documentation of each item, and whether the prospective Offeror will furnish such items with its own funds. The Offeror must identify Government-owned property in its possession and/or property acquired from Federal funds to which title vests in the offeror and that is proposed to be used in the performance of the prospective contract. The management and control of any Government property shall be in accordance with HHS regulations.

6. Additional Facilities - In the event the Offeror contemplates acquiring additional facilities in the performance of this work, such facilities shall be separately identified.

Other data required:

7. Financial Capacity - The Offeror shall indicate if it has the necessary financial capacity, working capital, and other resources to perform this contract without assistance from any outside sources. (If not, indicate the amount required, the anticipated source, and associated costs for such support.) The Offeror shall submit any information deemed relevant to convincingly demonstrate its ability to perform the requirement from a financial point of view; this will include providing a copy of the Offeror's most recent financial statement.

8. Commitments - The Offeror shall list commitments of key personnel with other clients/contracts and indicate whether these commitments will or will not interfere with the

completion of work and services contemplated to be completed under this contract.

9. Subcontractors – Specifically-identified subcontractors shall also submit a cost proposal fully supported by cost and pricing information and include a narrative to clearly describe in detail all supporting explanations of, or rationale for all proposed costs in the same manner as the prime Offeror, as detailed in 1 through 6 above.

L.10.5 DISCLOSURE OF LOBBYING ACTIVITIES

Standard Form LLL, "Disclosure of Lobbying Activities" can be accessed in the GSA Forms Library at: https://www.gsa.gov/reference/forms/disclosure-of-lobbying-activities

L.10.6 COST ACCOUNTING SYSTEM ADEQUACY

A completed Cost Accounting System Evaluation (Attachment J.1) must be completed and included as part of your business proposal.

L.10.7 ORGANIZATIONAL CONFLICT OF INTEREST DISCLOSURE/MITIGATION

Offerors are required to identify actual and potential organizational conflicts of interest (OCI) related to the services described in the statement of work for itself, as well as employees, consultants and subcontractors proposed. This includes, but is not limited to:

- The existence of conflicting roles that might bias judgment; and
- Access to nonpublic information that will give the offeror an unfair competitive advantage.

Offerors shall include an explanation of the process used to identify OCIs. If an actual or potential OCI is identified, the offeror shall submit a mitigation plan as part of its proposal. Offerors shall submit with their proposal an OCI affirmation, using the following language:

"I, (Name and Title), warrant that: 1) I am an official authorized to bind the entity; and 2) to the best of my knowledge and belief
"I, (Name and Title), warrant that: 1) I am an official authorized to bind the entity; and 2) to the best of my knowledge and belief

[ ] actual and potential organizational conflicts of interest have been identified and disclosed to the Contracting Officer (identify section of proposal) as of (Date)."

Or

[ ] no actual and potential organizational conflicts of interest exist as of (Date)."

L.10.8 INVOICE PROCESSING PLATFORM WAIVER REQUEST

Offerors may request a waiver from using the Department of Treasury Invoice Processing

Platform (IPP) for payment requests, which may be approved by the Contracting Officer for a specific situation, as follows:

- As specified in OMB Memorandum M-15-19, electronic invoicing is not appropriate for the Federal procurement: of relocation services, utilities, or for vendors using PII for identification
- Contractor is in the process of transitioning to electronic submission of payment requests but needs time to complete such transition. Contractor must indicate timeline for transition.
- Contractor demonstrates that electronic submission is unduly burdensome. Contractor must provide full explanation to include substantiating documents when necessary.

IPP waiver requests and supporting documentation shall be included in the business proposal.

L.9 PAST PERFORMANCE INFORMATION INSTRUCTIONS

Quoters will be evaluated on performance under existing contracts and performance on prior contracts. Quoters should note the difference between past performance and past experience. Past performance relates to quality and how well a contractor performed, while past experience is about the type and amount of work previously performed by a contractor.

Past performance information is available to Federal agencies through the Contractor Performance Assessment Reporting System (CPARS). The government will be considering past performance information contained in CPARS to the greatest extent possible.

A maximum of three (3) performance references shall be submitted for contracts under which performance has occurred within the past three (3) years. Past performance references can be for the quoter, predecessor companies, key personnel who have relevant experience and/or subcontractors that will perform major or critical aspects of the requirement when such information is relevant to the acquisition.

Each performance reference is limited to ten (10) pages and shall include the following information:

- Several points of contact (Contracting Officer, Contracting Officer's Representative and any other pertinent officials that can verify performance) - name, agency/company, address, phone number and email address
- For contracts with the Federal Government, indicate whether the government has evaluated the contractor and past performance information is available through CPARS or whether the reference will be providing information via the past performance questionnaire (see Attachment J.3)
- Contract title
- Contract number (and task order number when applicable)
- Contract type
- Total contract value (including base & all options)
- Project description and size information
- If the past performance reference is for a subcontractor, identify the major or critical

aspects of the requirement that they will perform
- Relevancy to the statement of work for the subject solicitation
- Did the contract include small business subcontract goals for small disadvantaged business concerns? If so, were the goals met?
- Provide an explanation of problems, delays, cost overruns and corrective actions taken.

In addition to the past performance information specified above:

For contracts that have performance information available through CPARS, quoters are requested to provide a copy of the CPARS report.

For contracts that do not have performance information available through CPARS, quoters are requested to provide the Past Performance Questionnaire (Attachment J.3) directly to their reference. The reference should complete the questionnaire and submit information directly back to the Government via email to Christopher.Poulos@hhs.gov by the close date of this solicitation.

Past performance information is proprietary source selection information. The Government will only discuss past performance information directly with the entity or person that is being reviewed. If there is a problem with the proposed subcontractor's past performance, the prime can be notified of a problem, but no details may be discussed without the subcontractor's permission.

SECTION M - Evaluation Factors for Award

M.1 52.252-1 SOLICITATION PROVISIONS INCORPORATED BY REFERENCE. (FEB 1998)

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

M.2 GENERAL

The Contracting Officer may eliminate from the competition any proposal that was not submitted in accordance with the solicitation instructions.

M.3 AWARD WITHOUT DISCUSSIONS AND COMPETITIVE RANGE DETERMINATIONS

The Government intends to evaluate proposals and award a contract without discussions with Offerors (except for clarifications as described in FAR 15.306(a)). Therefore, the Offeror's initial proposal should contain the Offeror's best terms from a cost or price and technical standpoint. The Government reserves the right to conduct discussions if the Contracting Officer later determines them to be necessary. In the event discussions are held, a competitive range determination will be made. If the Contracting Officer determines that the number of proposals that would otherwise be in the competitive range exceeds the number at which an efficient competition can be conducted, the Contracting Officer may limit the number of proposals in the competitive range to the greatest number that will permit an efficient competition among the most highly rated proposals.

M.4 BASIS FOR AWARD (TRADE-OFF)

The following factors will be considered in evaluating proposals, in descending level of importance:

- Technical;
- Cost;
- Past Performance

Award will be made to that responsible Offeror whose proposal contains the combination of those factors offering the best overall value to the Government utilizing the tradeoff process. This will be determined by comparing differences in technical merit and past performance with

differences in cost to the Government. The Government reserves the right to make an award to other than the lowest priced offeror or to the offeror with a higher technical score if the Contracting Officer determines that to do so would result in the best value to the Government. All evaluation factors other than cost or price, when combined, are significantly more important than cost or price.

Regardless of ratings on these factors, an award will not be made to an offeror that is ineligible due to an OCI (see L.# & M.#) or a determination of non-responsibility (see K.# & M.#).

M.5 TECHNICAL EVALUATION METHOD (TRADE-OFF)

The Government will evaluate the Technical Volume based on an Acceptable/Unacceptable evaluation criteria.

M.6 TECHNICAL EVALUATION CRITERIA

The criteria identified below will serve as the standard against which the technical proposal will be evaluated and identifies the significant factors which the Offeror should address in their proposal. The relative importance of the factors is:

M.6.1 FACTOR 1 - Technical Acceptability (Acceptable/Unacceptable)

Factor 1 will be evaluated on an Acceptable/Unacceptable basis. Each technical subfactor will also be evaluated on an Acceptable/Unacceptable basis. To receive an overall rating of Acceptable under Factor 1, the proposal must be rated Acceptable under all technical subfactors. This structure aligns with the integrated requirement for UCEDD and AT Program technical assistance, reporting and data systems, public-facing platforms, accessibility, and security/privacy.

Acceptable: The proposal demonstrates a clear, feasible, and compliant approach that meets the Government's minimum requirements and contains no material omission, deficiency, or failure creating unacceptable performance risk.

Unacceptable: The proposal fails to demonstrate a clear, feasible, or compliant approach to one or more material requirements, or contains one or more deficiencies, omissions, or material weaknesses such that the proposal is unacceptable for award.

M.6.2 SUBFACTOR 1 - Integrated Technical Approach (Acceptable/Unacceptable)

The Government will evaluate the extent to which the proposal demonstrates an acceptable approach for performing the integrated requirement, including coordinated, comprehensive, and specialized training and technical assistance to 67 UCEDDs and 56 AT Programs; delivery of tiered support ranging from broad-based and foundational assistance to targeted and individualized assistance for complex needs; support for statutory compliance, capacity building, program performance, peer exchange, dissemination, evaluation, and responsive problem-

solving; monthly reporting, performance monitoring, and annual evaluation support; and continuity, timeliness, and responsiveness across the full scope of work.

A proposal will be rated Unacceptable if it fails to address a material portion of the integrated UCEDD and AT Program requirement or fails to demonstrate a workable method for providing the required training and technical assistance services.

M.6.3 SUBFACTOR 2 Information Management, Data Systems, and Website Operations (Acceptable/Unacceptable)

The Government will evaluate the extent to which the proposal demonstrates an acceptable approach for operation and support of the required reporting and information management environments, including the UCEDD reporting platform and related web-based information management systems for Program Performance Reports (PPR), NIRS/PPR data, reporting support, dashboards, and public-facing UCEDD information management functions; AT data collection and reporting support, including ATRS, NATADS, or equivalent systems; annual reporting cycles; State Plan cycles; data validation and reporting support; maintenance and public dissemination functions for CATADA.info or an equivalent platform; continuity of operations; reliability; system support; issue resolution; and timely posting, updating, and public accessibility of required information.

A proposal will be rated Unacceptable if it fails to demonstrate a workable and reliable approach to maintaining and supporting the required UCEDD reporting platform, AT reporting and data functions, or website and public dissemination functions.

M.6.4 SUBFACTOR 3 Management and Staffing (Acceptable/Unacceptable)
The Government will evaluate the extent to which the proposal demonstrates an acceptable management and staffing approach for successful performance of the integrated requirement, including organizational structure and lines of responsibility; management of the combined technical, programmatic, operational, reporting, and website/platform functions; coordination and oversight of subcontractors and other team members; clarity of roles and responsibilities among the prime contractor and any proposed subcontractors; adequacy of prime contractor control and integration of subcontracted work; continuity of operations; responsiveness to Government, UCEDD, and AT Program needs; and, if applicable, the qualifications and availability of key personnel. The Government will consider whether the proposed management structure, staffing approach, subcontractor integration and oversight methods, and continuity approach are sufficient to support reliable performance across the full scope of work.

A proposal will be rated Unacceptable if the proposed management approach, staffing, or subcontractor integration and oversight appears insufficient to perform the integrated scope of work.

M.6.5 SUBFACTOR 4 Accessibility, Security, and Privacy (Acceptable/Unacceptable)
The Government will evaluate the extent to which the proposal demonstrates an acceptable approach to meeting applicable accessibility, security, and privacy requirements, including

Section 508 and WCAG 2.1 Level AA compliance; accessibility review and remediation processes; protection of federal information and systems; secure operation of public-facing systems and websites; and coordination with Government personnel on information security and privacy matters.

A proposal will be rated Unacceptable if it fails to demonstrate a compliant and workable approach to these requirements.

M.6.6 FACTOR 2 – Price

The Government will evaluate price for completeness, reasonableness, balance, and arithmetic accuracy.

The total evaluated price will include all CLINs, option periods, and any evaluated optional tasks identified in the solicitation.

A proposal may be rejected if the Government determines that pricing is materially unbalanced or otherwise reflects a lack of understanding of the requirement.

M.6.7 FACTOR 3 –INFORMATION AND COMMUNICATION TECHNOLOGY ACCESSIBILITY (ACCEPTABLE/UNACCEPTABLE)

Supplies - The completed Accessibility Conformance Report (ACR) will be assessed as to whether proposed ICT supplies, products, platforms, information, and documentation meet applicable Section 508 accessibility standards.

Services – The response will be assessed as to whether proposed ICT services conform to Section 508 accessibility standards.

If ICT does not conform and cannot be acceptably remediated, rationale for an exemption or exception must be provided. Potential exemptions and exceptions are identified in FAR subparts 39.204 and 39.205. The government determines whether an exemption or exception can be appropriately applied.

This factor will be evaluated as Acceptable or Unacceptable.

M.7 PAST PERFORMANCE EVALUATION

Past performance information is one indicator of an offeror's ability to perform the contract successfully. This evaluation is subjective and will be based on information obtained from references provided by the offeror, as well as information obtained by other sources known to the Government. For the purpose of this evaluation the term "offeror" is inclusive of the prime, predecessor companies, key personnel and subcontractors for which past performance will be evaluated.

The Government will consider the relevancy and quality of the offeror's past performance to assess the risk of unsuccessful contract performance. If quality information is not available for a reference, the reference will not be evaluated for relevancy, nor considered in determining the overall risk rating.

STEP 1 - Relevancy

Each reference will be evaluated for relevancy based on the scope and magnitude of effort and complexities of the work performed and how it compares to the services specified in Section *** of this solicitation.

Rating	Definition
Very Relevant	Performance effort involved essentially the same scope and magnitude of effort and complexities this solicitation requires.
Relevant	Performance effort involved similar scope and magnitude of effort and complexities this solicitation requires.
Somewhat Relevant	Performance effort involved some of the scope and magnitude of effort and complexities this solicitation requires.
Not Relevant	Performance effort involved little or none of the scope and magnitude of effort and complexities this solicitation requires.

STEP 2 - Quality

To determine how well the offeror has performed in the past, the Government is using past performance rating information available in CPARS, information provided by references, as well as information obtained by other sources known to the Government.

Each reference will be evaluated for the overall quality of the performance.

Rating	**Definition**
Excellent	The contractor has performed successfully and greatly exceeded expectations under the contract.
Good	The contactor has performed successfully and exceeded expectations under the contract.
Acceptable	The contactor has performed successfully under the contract.
None	No record of performance or performance is inconclusive

Mediocre	The contractor has some unsuccessful performance under the contract.
Deficient	The contractor has performed unsuccessfully under the contract.

STEP 3 - Risk Rating

After considering the relevancy and the quality of the offeror's past performance, an overall risk rating will be determined for each offeror. The risk rating is an assessment of the overall risk of unsuccessful contract performance based on the past performance of the offeror. The more relevant the references are to the current acquisition, the more significant the reference becomes and the more weight it is given in determining the risk rating. Adverse past performance information on references that are not deemed to be relevant may be taken into consideration in determining the risk rating if the adverse information is considered to have bearing on the current acquisition. The Government will consider the type and amount of work to be performed by the prime, key personnel, and major or critical subcontractors to determine the significance of their past performance information when determining the risk rating. In the case of an offeror without a record of relevant past performance or for whom information on past performance is not available or is inconclusive, the offeror will not be evaluated favorably or unfavorably on past performance.

Rating	Description
Unknown Performance Risk	No performance record is identifiable, past performance is not relevant to the required effort, or the past performance information is inconclusive
Very Low Performance Risk	Based on the offeror's performance record, no doubt exists that the offeror will successfully perform the required effort
Low Performance Risk	Based on the offeror's performance record, minimal doubt exists that the offeror will successfully perform the required effort.
Moderate Performance Risk	Based on the offeror's performance record indicating some unsuccessful contract performance, some doubt exists that the offeror will successfully perform the required effort.
High Performance Risk	Based on the offeror's performance record indicating unsuccessful contract performance, substantial doubt exists that the offeror will successfully perform the required effort.

M.8 PRICE/COST EVALUATION (Cost Reimbursement)

The price/cost proposal will be evaluated for reasonableness. For a price to be reasonable, it must represent a price to the government that a prudent person would pay when consideration is given to prices in the market. Normally, price reasonableness is established through adequate price competition, but may also be determined through cost and price analysis techniques as described in FAR 15.404.

A cost realism analysis will be conducted to determine if:

(a) The offeror's proposed costs are realistic for the work to be performed;
(b) The proposed costs demonstrate that the offeror understands the Government's requirements; and
(c) The proposed costs are consistent with the various elements contained in the technical proposal and other portions of offeror's business proposal

M.9 PROSPECTIVE CONTRACTOR RESPONSIBILITY AND ELIGIBILITY STANDARDS

Failure by the offeror to affirmatively demonstrate adequate compliance with the general standards of prospective contractor responsibility at FAR 9.104-1, and any special standards established for this acquisition under FAR 9.104-2, may result in a determination of non-responsibility. As with all aspects of prospective contractor responsibility, a finding of non-responsibility can be made at any time prior to contract award. Per FAR 9.103(b), if the prospective contractor is a small business concern, responsibility will be determined in accordance with Subpart 19.6, Certificates of Competency and Determinations of Responsibility. If the prospective contractor is a Section 8(a) participant, see Subpart 19.8.

M.10 ORGANIZATIONAL CONFLICT OF INTEREST

If the Government determines that an organizational conflict of interest (OCI) exists, that cannot be satisfactorily avoided, neutralized or mitigated or waived, the Contracting Officer may determine that the offeror will not be eligible for award. The Government reserves the right to only consider mitigation plans proposed by the apparent successful offeror. If this acquisition is governed by FAR Part 15, the process of approving an OCI mitigation plan and revisions to such a plan does not constitute discussions as described in FAR 15.306.