1. Purpose

The purpose of the SOO is to obtain contractor support with the knowledge, skills and abilities for supporting the Centers for Disease Control and Prevention (CDC), Office of Science (OS), Knowledge Management (KM) and with the implementation of the KNOWLEDGE MANAGEMENT TECHNICAL SUPPORT SERVICES (KMTSS).

2. Scope

This SOO addresses work associated with the following KMTSS activities:

1. Provide IT product design, development, enhancement, and operations and maintenance support that includes a DevSecOps approach to the following: help desk, quality assurance, data cataloging, agile software development, systems and software deployment, systems operations, information management, and enterprise data capabilities.
2. Seeks multi-functional, full stack agile software development teams qualified to provide the required IT Capabilities to Knowledge Management across the portfolio of activities identified in the Statement of Objectives (SOO).
3. Provide expert support for open science initiatives at CDC including scientific data, publication, and code release.
4. The SOO tasks are outlined and detail the IT products and services needed. All IT products and services delivered must be consistent with the CDC EPLC guidelines.
5. Knowledge Management will identify product owners to interface with industry requirements management teams and support the agile development process for each IT product and service.

3. Period and Place of Performance

PERIOD OF PERFORMANCE:

BASE PERIOD: September 30, 2026 – September 29, 2027 (12 Months)
OPTION PERIOD ONE: September 30 , 2027 – September 29, 2028 (12 Months)
OPTION PERIOD TWO: September 30 , 2028 – September 29, 2029 (12 Months)
OPTION PERIOD THREE: September 30 , 2029 – September 29, 2030 (12 Months)
OPTION PERIOD FOUR: September 30 , 2030 – September 29, 2031 (12 Months)

PLACES OF PERFORMANCE:

Teleworking is both permitted and preferred.
When on site work is required work is to be performed in a normal office environment.
Hours of operation 8:00am to 5:00pm with extended hours for KM Help Desk. When on site work is required, the majority of the work will be accomplished in Atlanta, GA in the government facilities listed below.

Atlanta Locations:

Roybal Campus	1600 Clifton Road Atlanta GA 30333
Chamblee Campus	4770 Buford Highway Chamblee, GA 30341
Century Center	Campus Century Blvd. Atlanta, GA 30345
Corporate Square	Campus Corporate Square Campus 30341
District at Chamblee	Brandywine Road Atlanta, GA 30341

4. Background

4.1 OVERVIEW OF KEY OFFICE OF SCIENCE / KNOWLEDGE MANAGEMENT SERVICES

The Centers for Disease Control and Prevention (CDC), Office of Science (OS), Knowledge Management (KM) designs, develops, deploys, supports, and enhances a portfolio of public and internally facing enterprise business information systems for CDC and its partners. Over the past several years, Knowledge Management has expanded

its portfolio to provide IT solutions and services to CDC's Centers Institutes and Offices (C/I/Os) as well as the United States Department of Transportation (USDOT), the National Oceanographic and Atmospheric Administration (NOAA), the Federal Deposit Insurance Corporation (FDIC), and the Minority Business Development Agency (MBDA). The applications in this portfolio must continuously respond to changing user needs and evolve in a technically sound and efficient manner. It is also vital that the KM system have the ability to harvest as well as share data with a number of CDC systems. The core applications to Knowledge Management are eClearance, Publishing Reporting, CDC Stacks, and the Data Scanning Tool.

4.2 ROLE OF CONTRACTORS IN EXECUTING KEY KM SERVICES

The Knowledge Management team was established to provide help desk, quality assurance, application development, data management, operations support and related services across this portfolio of applications for the purpose of providing high quality, reliable, and available software featuring advanced functionality. The products and services developed, managed, and maintained by Knowledge Management are used across CDC and directly support numerous important CDC centers and groups in achieving the Agency's public health objectives. As public health missions and needs evolve, Knowledge Management must continually monitor and update its software and information management capabilities to meet those needs.

Knowledge Management operations are supported, in part, by Contractor personnel tasked with a full range of support functions across the application development lifecycle and consistent with CDC's implementation of the HHS/CDC Enterprise Performance Lifecycle (EPLC). KM utilizes an Agile framework to continuously evaluate and improve the efficiency and effectiveness of its applications and seeks a Contractor who will bring experience-based perspective to the blending of the multiple technologies needed for delivery of the portfolio of KM applications.

4.3 MODERNIZATION EFFORTS

The Knowledge Management modernization roadmap is not a standalone effort. It aligns with, supports, and interfaces with other enterprise modernization efforts including:

- **CDC AI Strategy** – Knowledge Management is leading the way for CDC's use of Artificial Intelligence in both the development of the systems as well as improving the support KM provides authors, scientists, and other CDC staff
- **CDC Public Health Data Modernization Initiative** - the purpose of which is to improve data collection and analysis using innovative and interoperable data collection and analysis technologies. The Knowledge Management group is a leading element in the CDC's implementation of new Data Use Agreements (DUA)
- **CDC Gold Standard Science Strategy –** Knowledge Management supports the administration's goal of gold standard science at CDC. With the core tennet of scientific transparency, KM provides assistance with the release of scientific data and code associated with CDC publications.
- **System Connections** – Interoperability is a core tenant of the KM systems. This requires KM systems to both send and receive data from a number of CDC as well as external systems.

5. Knowledge Management KMTSS Objectives:

- Provide application planning, design, development, testing, deployment, operations, maintenance, help desk and enhancement services in a manner consistent with the HHS/CDC EPLC and utilizing application development best practices such as Agile development;
- Provide these responsive, efficient, and cost-effective IT application support services in compliance with appropriate technical and security requirements and considerations;
- Evaluate, analyze, design, configure, maintain, develop, implement, support, and document business and information requirements and needs to support automation of software and information management capabilities;

- Support CDC staff, including programmers, statisticians, analysts, center administrators, executives, public affairs officers, and information specialists in using Knowledge Management applications and services;
- Advise Knowledge Management in all areas of application development, operations, and maintenance including technology and application trends and directions, upgrades and enhancements;
- Evaluate, recommend and implement new advances in business and scientific applications, data management, application delivery, tools and technology.

6. Task Order Objectives, Contract Administration and Functional Support Areas

6.1 TECHNICAL OBJECTIVES

6.1.1 **AI usage.** The contractor shall ensure the proper use of AI tools in all aspects of system development and support based on HHS and CDC guidelines.

6.1.2 **Replacement of Documentum/OpenText.** The contractor will continue to support the migration away from the Documentum/OpenText backend system to a more data driven platform.

6.1.3 **Systems Support.** The contractor shall support all of the Knowledge Management software and systems infrastructure. This includes all aspects of the system development lifecycle including the updates necessary to support CDC's Cloud Strategy. The contractor will be required to have detailed knowledge of the software stack, both onsite and AWS systems environments, and operational duties necessary to run Knowledge Management systems without significantly increasing Capability cost, hindering Capability performance (no degradation in performance) or lengthening schedule (no more than 2- week delay)..

6.2 CONTRACT ADMINISTRATION AND MANAGEMENT.

The contractor shall provide administrative and management support as outlined below. This support is considered integral to the management and execution of the contract.

a. *Contract Management and Administration*. The contractor shall identify a single point of contact for all official communication regarding performance and communicate this POC's information to the government PM, COR and contracting officer. The contractor shall respond to Government requests in a timely fashion, generally the same day of the request, with either the requested information OR the date the information can be reasonably provided. The contractor shall make travel arrangements for its employees if travel is required by the government.

b. *Contract Administration Related Meetings.* The contractor shall schedule and hold meetings with the COR to discuss contract related items, such as deliverables, performance, quality, and progress. These meetings will typically occur monthly or on an as needed basis per recommendation by the COR. The contractor shall provide the COR meeting materials including, but not limited to, an agenda, at least two days before the date and time of the meeting. This responsibility may be delegated by the COR to a technical monitor or other appropriate staff member.

c. *Status Reports.* Submit a Monthly Status Report no later than the fifth business day of the succeeding month that provides a narrative regarding, as applicable to core and/or exercised optional requirements, testing planned and executed, test results, automated test code coverage, test-related metrics, progress on key projects, metrics, bugs/fixes status, AIR application downtime, status of pending documents and/or deliverables, progress on sprints, next major milestones, status of significant contract management issues such as personnel vacancies, significant risks or concerns, and government support required to enhance performance. Additional technical updates or reports may be required.

d. *Orientation Briefings*. Within one week of award, the contractor will request to schedule an initial orientation briefing with the government. The orientation briefing will be held at a location and date and time mutually agreed upon by both parties, or remotely. At the briefing, the contractor will outline

the approach and schedule for the requirement as well as address the control and management mechanisms they will use to oversee their work. The contractor will also identify key and supporting personnel and sub-contractors' firms that will be used to accomplish the tasks. As applicable, the briefing should also address contractor transition items such as recruiting, retention of incumbent personnel, roles and responsibilities of key personnel on the contractor's staff, task order communication management (means, methods, frequencies, and responsibilities), security, badging, onboarding, etc., including a milestone chart.

e. *Meetings and Coordination.* Participate in internal and external meetings, stand-ups, conference calls, and engagements as required for performance. Participation is active, engaged, and value-added. Contractor personnel with the appropriate skills and experience are identified to participate. As required, schedule, coordinate, prepare for, assist with, and support meetings. Prepare agendas, disseminate preparatory materials, and prepare meeting summaries and/or minutes along with tracking assignments / action items, their status and completion. Apply subject matter expertise to determine relevant topics, agendas, and determine functional and technical content.

f. *Briefings.* Prepare, develop, design, update, revise, and maintain briefings as required for performance. Be prepared to brief senior leaders and senior executives on within-scope topics as needed.

g. *Contract Kick-Off.* Within 10 business days of award, the contractor shall meet with relevant OAS and KM personnel to review and clarify the scope of work and delivery schedule for this contract and address contractual matters (e.g., invoice procedures). In consultation with KM, the contractor shall develop, prepare and distribute an agenda 2 days prior to the Kick-Off Meeting.

    a. Discussion topics may include, but are not limited to the following:
    b. Review of program purpose, goal, functional areas, and expected products;
    c. A discussion of the program management approach;
    d. An overview of existing program issues, include transition from the incumbent contractor to the new contractor;
    e. Development of the performance plan to guide the overall direction of the program, including identification of both program and project risk and proposing risk mitigation strategies;
    f. A discussion of the format and timetable for deliverables;
    g. A review of the program governance strategies including requirements tracking, project scope, cost, schedule, and performance management; and
    h. Any other questions or issues identified by the Contractor.

6.2.1 **Transition Out.** The Contractor shall plan and implement a transition from the incumbent to the incoming contractor/government personnel at the expiration of the contract. This includes coordination with Government staff and/or successor contractor staff. Provide a Transition Plan no later than 180 days prior to expiration of the contract for government inspection/acceptance. The Plan must identify at a minimum how the contractor will transfer the following:

1. Points of contact established with KM customers
2. Location of documentation, archives, artifacts, procedures, models, etc.
3. Transfer of source data or code for current and developing Capabilities
4. Transfer of files, in a coherent and organized manner, from corporate servers and individual accounts related to completed Capabilities
5. Status of ongoing work
6. Appropriate contractor to contractor coordination to ensure a seamless transition
7. Transition of personnel, if applicable
8. Transition schedule and milestones
9. Identify actions required of the Government
10. Inventory of software licenses, warranties, maintenance agreements, customer accounts associated with KM software, product keys, and installation discs and packaging.

At the end of the task order term, the electronic copies of all materials acquired, developed and operated as part of the contract, shall be delivered to the COR. The contractor, at the direction of the COR shall develop a transition plan that includes a process and schedule for the transition of materials acquired, developed, and operated during the period of performance of the contract, to be reviewed and approved by the COR not less than six 6) months before the end of the period of performance for the contract. The contractor shall provide necessary information and consultation to the new contractor on the design, management, and operation of such materials, upon delivery. The transition will be complete when the COR approves, in coordination with KM that all materials acquired, developed, and managed during the period of performance have been transferred to KM in readable and executable form.

6.3. FUNCTIONAL SUPPORT AREAS

6.3.1 **Project Management**. KM has developed a robust project management process to track project progress and manage project financials. The contractor team will be responsible for managing various types of KM projects (e.g., eClearance, STARS, CDC Stacks. SWAT, Publishing Reporting etc.). To support KMs project management requirements, the contractor will be responsible for developing project management artifacts in the JIRA system for each project, to appropriately tailor HHS/CDC EPLC framework rigor to the project requirements. In addition, the contractor will develop plans for each of these aspects of project management, while managing the balance across them as changes occur throughout the project lifecycle.

The contractor will also be responsible for developing detailed project schedules in KM's project management system of record JIRA including all required project tasks, assignment of resources to all project activities, and tracking actual work performed on each task within the tool. The contractor must provide actual hourly rates of every team member for the purposes of estimating project costs, tracking actuals, and automating the reporting of cost variances within the project management tool.

In addition, the contractor will be responsible for producing all Project Management documentation in accordance with HHS/CDC EPLC and KM guidance as well as monitoring and reporting on project status and milestones in regular project status reviews/reports. The contractor will be responsible for escalating high-impact risks to the KM COR to facilitate mitigation.

Principal Tasks to be performed by the contractor shall include:

a. Performing project initiation
b. Performing project planning
c. Gaining approval of Business Need Statement within 10 days of project activation
d. Develop Project Management Plan
e. Develop and manage project scope,
f. Performing design and development;
g. Executing testing;
h. Executing implementation;
i. Manage and maintain project-specific SharePoint sites and associated content;
j. Managing project risks and issues;
k. Reporting project status and metrics;
l. Ensuring successful project delivery;
m. Performing project change management via Project Change Requests;
n. Ensuring Sprint Ceremonies are held
    i. Conduct Sprint Planning meetings before the start of each sprint, gaining Product Owner approval Conduct Sprint Reviews at the end of each sprint, gaining Product Owner approval
    ii. Conduct Sprint Retrospective at the end of each sprint with project team
    iii. Conduct Project Retrospective at the end of each project
o. Conducting project kick-offs within 10 days of project activation for development, modernization and enhancement projects

p. Providing Stage Gate deliverables at least 15 days prior to the Stage Gate
q. Conducting project schedule baselines within 5 days of project activation or within 5 days of gaining Baseline Stage Gate approval
r. Developing Closeout Reports and the end of each project

6.3.2 Knowledge Management Systems

KM has three primary enterprise systems:

1. **Document Operations and Clearance System (DOCS)** is a system built on top of Documentum and encompasses four functional applications or workflows.
   a. **eClearance** – This provides the workflow and approval process necessary to support the clearing of publications prior to publication or distribution. This can include journal articles, pamphlets, posters, videos, and/or audio clips
   b. **Data Use Agreements** - This supports the workflow and approvals for agreements that include the CDC as a whole with external parties. The objective of these agreements is to allow individual data scientists to have access to data from, or share data with, an external source without having to create an individual agreement.
   c. **STARS** – This supports the workflows for Data Management Plans, Paperwork Reduction Act filings, and Human Subjects clearance.
   d. **Publishing Reporting** – This system provides reporting related to publication statistics and workflow status for center administrators and divisional management officials.
   e. **Tipster** – Built on JIRA, this system provides helpdesk ticketing and development feature tracking for KM projects. It also serves as the main tool for tracking the Agile sprints.
2. **CDC Public Access Platform (CPAP)-** An AWS deployed application environment that is replicated for other Federal Agencies. CDC, FDIC, NOAA, and USDOT are currently supported; however, support for additional Federal Agencies may be added during the period of performance.
   a. **Stacks** – This is the front-end, anonymous access, public website that supports the distribution of publications. It includes cataloging data, meta-data and the digital retrieval of such through the OAI-PMH open standard. All distributed documents are full-text searchable and include historical versions (if historically updated and the historical version is still available).
   b. **SWAT -** The Stacks Workflow Administration Tool is the back-end administration interface for CPAP. The system is PIV only authentication and requires integration with CDC, FDIC, NOAA and USDOT PIV issuance certificate authorities. SWAT is used by the data catalogers to create/manage catalogs, upload documents and manage the supporting metadata for the documents.
3. **CDC Vault** – An non-public version of CPAP that requires all users to be PIV Authenticated. This supports MODERATE rated catalogs of data for internal, non-public use. This also includes a section for data being preserved as federal records and the automated migration of those records to the National Archives and Records Administration (NARA) based on the record retention schedule for each specific document.
4. **Data Scanner –** The data scanner is a tool that allows any staff member at CDC to scan a document for PII or other sensitive information before being released to the public. This system is built using Ground Labs as the backend engine with a custom front end for an easier user interface.

Knowledge Management supports an Agile sprint schedule for developing, quality testing, and security testing functional updates on a ad-hoc basis, focusing on ensuring high quality and timely releases to agency staff.

The backlog of enhancements for each platform will be prioritized and decisioned on a per sprint basis via status meetings with critical stakeholders and users.

To support the continued growth of KM's systems, the contractor will be responsible for partnering with KM to review prioritized platform enhancements and determining implementation timelines. KM

and the contractor will review each platform's short, and long-term release plans during sprint review meetings, to review progress against development budgets, technical risks, changes in priorities, and technical roadblocks.

The contractor will also be responsible for providing technical solution architects to partner with KM's technical staff to define the strategic business and technical roadmaps for each platform.

Principal Tasks to be performed by the contractor shall include:

a. Providing dedicated full stack DevSecOps teams that can manage the full lifecycle of the systems, from development, testing, security, deployments, and infrastructure.
b. Ensuring that development work aligns KM's goals for systems consolidation and modernization, as defined by our modernization roadmaps.
c. Ensuring that each platform releases high-quality, function releases.
d. Ensuring that each release conforms to integrate latest federal requirements (508, security, etc.)

6.3.3 **User Experience and User Design.** KM envisions User Experience and User Design to encompass both usability and accessibility. This includes meeting WCAG 2.0/2.1 AA success criteria and complying with Section 508 of the Rehabilitation Act for ACL services, systems and websites, and other digital content.

The contractor shall ensure that service and system development, enhancement, and operations work includes user experience and user design participation and review. UX and UD deliverables may include design options represented as wireframes; design standards for systems and websites; design standards for UX support on mobile device platforms; and other documents that both the customers and development team can use to review, approve, and incorporate into systems and websites. The contractor shall work with KM staff to ensure all new and enhanced systems, services, and websites are tested for and meet WCAG 2.0/2.1 AA success criteria and have been assessed and evaluated by users interacting with the system with assistive technology such as screen readers or voice interaction tools.

The contractor may review and report on other work products or materials that include but are not limited to documents, presentations, webinars, and audio and video content for distribution, applications, and systems, with meeting WCAG 2.0/2.1 AA success criteria and complying with Section 508. The contractor shall also work with KM staff to ensure automated accessibility testing of systems, services, and websites. Finally, the contractor shall utilize usability testing and analysis on systems that have been in production to identify potential enhancements that inform future releases.

Principal Tasks to be performed by the contractor shall include:

a. Performing User Interface design for desktops and mobile platforms;
b. Promoting and enabling Section 508 compliance;
c. Participating in User Interface design reviews;
d. Developing automated 508 and quality testing;
e. Performing usability testing; and
f. Participating in project planning activities.

6.3.4 **Application Design/Development.** KM has three major system designed, developed on multiple technology platforms. The primary development platforms and technologies include:

- IIS
- Apache Web Server
- Apache Tomcat
- Java
- PHP
- Python

- MySQL
- Microsoft Server (2012, 2016, 2019)
- Microsoft SQL (2016, 2019)
- Red-Gate
- MS Visual Studio
- Eclipse
- Documentum
- Opentext
- SOLR
- Drupal
- Islandora
- Jenkins
- GIT
- SVN
- MediaWiki
- Chef Automate
- PRTG
- Splunk
- Groovy
- Katalon
- Apache JMeter
- Microsoft Power Shell
- ERStudio
- Visio
- Kubernetes
- Docker

When developing or performing major enhancements to KM applications, the contractor will ensure that all systems conforms to all current or future CDC and KM technical standards and guidelines.

The contractor will also be responsible for working with KM customers to document requirements, business rules, and process workflows. The contractor will also be responsible for defining user stories based upon customer requirements, which can be converted into technical or system requirements.

The contractor technical team will also be responsible for working with KM business, technical and security stewards to ensure that the technical designs meets KM and CDC technical standards, and that any additional software packages or technologies are approved for use by KM and the CDC.

As part of the development and enhancement of KM systems, the contractor will be responsible for meeting the automated testing code coverage requirements defined by KM for each system. KM will provide the contractor guidance on automated testing code coverage goals on a system-by-system basis.

KM has implemented automated code quality checks into system releases using SonarQube. The contractor will be responsible for meeting the code quality score set by KM for each system and ensuring that the code quality score improve with each release.

KM has also invested in automated security scanning tools that evaluate each system for security vulnerabilities during each release. The contractor will be responsible for ensuring that all identified security vulnerabilities are mitigated prior to any production releases of a system. The contractor will also ensure that all systems updates comply with federal 508 standards for accessibility.

Principal Tasks to be performed by the contractor shall include:

a. Coordinating, contributing to, managing, and maintaining required application documentation, including but not limited to:
    1) Business rules
    2) Access Control rules and framework
    3) User stories with Acceptance Criteria
    4) User Interface Wireframe/Mockup
    5) Activity Diagrams/Analysis Assets
    6) Process Flow Diagrams
    7) Non-functional requirements
    8) Technical design documents
    9) User Guides, as needed
    10) Configuration Management Plan, as needed
    11) Operations and Maintenance Plan
    12) Disposition Plan
b. Working with Business, Technical, and Security Stewards to ensure application is developed in accordance with CDC and KM architectural principles
c. Developing automated unit and integration tests that meet KM's code coverage goals per system
d. Developing applications that adhere to 508/WCAG guidelines for compliance
e. Developing applications that meet CDC mandated security requirements
f. Developing applications that meet code quality standards defined by KM
g. Identifying / correcting application performance bottlenecks and optimizing data access
h. Developing Records Management processes and mechanisms to manage records retention as mandated by Records Management Policies

6.3.4.1 **Application Quality Control**

The contractor will also be responsible for regular regression testing of applications to ensure that changes to the code, environment or hardware have not impacted the associated applications. The contractor is required to include regression testing with each code update. The contractor shall be responsible for the development and execution of fully automated regression tests, using Groovy defined tests with Katalon, manual testing and performance tests using Apache JMeter.

To support KM's production support activities, the contractor will be responsible for monitoring application defects or enhancement requests reporting by customers through the Knowledge Management helpdesk or other channels. The contractor will be responsible for reviewing system change requests with KM management for prioritization and partnering with KM to determine implementation timelines.

Principal Tasks to be performed by the contractor shall include:
a. Performing systems quality analysis and troubleshooting for application defects and performance issues
b. Performing application releases
c. Performing regression testing;
d. Performing performance testing of the core KM systems

6.3.4.2 **Application Release Management.**

For systems development, the KM is modernizing its system release processes to take advantage of Dev DevSecOps release automation best practices.

The contractor will be responsible for the creation and maintenance of automated systems deployment workflows through the KM's release management tools Jenkins and Terraform. The contactor will

also be responsible for the automation of all required release approvals, as defined by KM or OCISO change management processes. The contractor will be responsible for the integration and automation of system security and testing technologies as part of the release pipeline.

When scoping and prioritizing application releases, the government will provide guidance. Although maintenance releases do not necessarily need to follow the Stage Gate Review process of formal projects, the Contractor shall keep all application documentation up to date to reflect the changes in the maintenance release.

Principal Tasks to be performed by the contractor shall include:

a. Preparing production and maintenance releases for approval
b. Planning release windows
c. Measuring and monitoring maintenance release progress
d. Developing and executing deployment plans and implementation plans
e. Coordinating go-live activities
f. Developing release reports
g. Participate in post-implementation reviews

6.3.5 **Knowledge Management Helpdesk and Training** KM's informatics workstream focuses on providing workflow support to CDC scientists, authors, and administrators by through the use and operation of Knowledge Management tools and services

In order to support the KM's helpdesk activities, the contractor will be responsible for providing staff who are subject matter experts in Knowledge Management systems and are capable of interacting with both customers and directly addressing the problems with KM infrastructure (such as Microsoft SQL).

In addition, the contractor will be responsible for creating the training material and offering regularly scheduled, instructor lead, training classes for users of KM systems. The training will cover the proper use and expectations for DOCS and it's subsystems for internal users and SWAT for both internal users and users from partnered federal agencies.

Principal Tasks to be performed by the contractor shall include:

a. Providing helpdesk based Subject matter/ domain expertise of Knowledge Management systems. .
b. Facilitating Stakeholder and external partner training coursework and instructor lead classes

6.3.6 **KM Operations.** KM has a predominantly CDC cloud infrastructure hosted environment. The contractor will need to coordinate and often lead work done by the Applications Hosting Brach and Network Technology Branch for all KM infrastructure such as the containerized environment and the server-based systems. For the containers, the contractor will need to support the creation, maintenance, security and monitoring of the terraform deployment and the associated container images. The contractor will ensure that the environment conforms to all security policies and standards. In addition, the contractor will provide support for the creation, maintenance, and monitoring of server-based KM resources, including web servers, application servers, database servers, and support servers. The contractor will ensure that each server performs optimally and are designed to minimize unscheduled downtimes. The contractor will be responsible for the creation and monitoring of on-premise infrastructure dashboards, resolving performance and functional issues, and ensuring infrastructure software and servers are patched with the latest software versions and security updates.

For KM's cloud infrastructure, the contractor will be responsible for providing cloud architects with knowledge of AWS and Azure to support cloud infrastructure solutions. The contractor will design and deploy cloud infrastructure solutions with server-less technologies when available and develop infrastructure as code and automated software deployment as appropriate. The contractor will also be responsible for supporting the KM with cloud management tasks, such as cost optimization, infrastructure monitoring, infrastructure support and cost projections.

For both the on-premise and cloud infrastructure, the contractor shall create and maintain infrastructure design documents and document all changes that occur through infrastructure change requests.

Principal Tasks to be performed by the contractor shall include:

a. Administration of websites, container images, cloud resources, virtual machines, and servers
b. Administration of cloud networking, including VPCs and Hybrid Cloud Networks, and integration with the HHS and CDC networks
c. Creation and maintenance of monitoring solutions for infrastructure and applications
d. Performing systems analysis and troubleshooting for on-premises and cloud infrastructure
e. Designing and implementing infrastructure, both on-premises and in the cloud, to support KM's systems and services
f. Performing impact analysis of infrastructure updates and changes
g. Performing analysis on configuration defects found in the production environment;
h. Performing and supporting maintenance releases;

6.3.7 **Database Operations and Maintenance Support.** The KM primarily utilizes Microsoft SQL Server technologies but does have MySQL and PostgreSQL for some specific open-source software stacks. The contractor will be required to create, design, and manage both on-premises and cloud-based databases. The contractor will be required to monitor the health of the database environment, maintain cross-country replication, manage and support data ingest processes, support developer coding efforts and helpdesk service tickets, and stay current with database security both industry standard and CDC specific.

The contractor will be responsible for responding to database issues, incidents, and problems reported through the KM help desk. This includes the day-to-day tasks of assuring database availability, optimizing databases for performance and efficiency, and ensuring proper security and authorized access to database objects and data.

The contractor will also be responsible for reporting on environmental inconsistencies between each database environment (development, testing, UAT, training, staging, and production), and coordinating database change management with the operations and development teams.

Principal Tasks to be performed by the contractor shall include:

a. Adhere to all data management security rules and processes (e.g., authentication, authorization, encryption, auditing, and intellectual property).
b. Propose, develop and implement enhancements to security rules and processes.
c. Adhere to database management processes and procedures.
d. Propose, develop and implement enhancements to database management processes and procedures.
e. Ensure data is managed and maintained to support records management criteria.
f. Ensure database production environment meets all up-time requirements and identify potential impacts and solutions that may result in database production downtime.
g. Ensure business continuity of database management environment to include, but is not limited to high availability, disaster recovery and migrations and upgrades.
h. Monitor and troubleshoot development, testing and staging servers for deadlocks, performance issues and resource issues.
i. Performance tune queries and offer expertise on set-based operations
j. Performance tune onsite and cloud based database servers and identify and resolve system bottlenecks
k. Offer consulting on optimal architecture and data model
l. Eliminate obsolete database objects and configuration settings.
m. Evaluate error, audit and transaction logs to identify issues or areas of concern.
n. Evaluate and implement performance improvement techniques (e.g., indexing, database checkpoints, etc.) to prevent long running or inefficient queries.
o. Ensure appropriate creation and management of database transaction-logs.

p. Evaluate data for accuracy, relevancy and consistency.
q. Detect, analyze, and resolve data quality issue(s).
r. Create and manage data modeling and normalization to ensure that databases are designed to promote data integrity.
s. Observe data quality standards to safeguard data integrity and data value.

6.3.8 **Communications**. The contractor will provide communications support across all KM applications. As application new releases are rolled out or experience issues, the contractor will support KM by providing communication support for stakeholders and systems users. In addition, the contactor will support keeping Publishing Assistant content current for KM.

Principal Tasks to be performed by the contractor shall include:
a. Developing communications plans for projects and production systems;
b. Providing communications coverage during the KM Helpdesk established support hours;
c. Assisting with the maintenance/modification of application training and use content on the Publishing Assistant site.
d. Documenting and maintaining communication processes, procedures, and templates updated at least quarterly.

6.3.8.1 *Reports Development.* The contractor shall develop application reports required to generate data and information for new/updated and enhanced applications. This development is for the generation of canned or custom reporting interfaces to support development projects. As part of application development efforts, reports developers are responsible for supporting data warehouse integration efforts. The contractor shall also support and perform various types of standard and non-standard reporting including ad-hoc reporting and self-service reporting.

6.3.8.2 *Documentation.* The contractors shall document as appropriate the design, architecture, infrastructure, and operating and user guidance for applications, services, systems, and websites it develops and operates under this SOW. The contractor shall ensure its documentation is accurate, free of jargon and typographical errors, and meets KM's requirements for accessibility and usability. The documentation shall be maintained according to formats specified by CDC project leads and stored in a CDC document management repository.

6.3.8.3 *Training.* The contractor shall develop simple, easy to use training materials in support of the services, systems, applications and websites developed and operated in the other objectives and tasks. The contractor may be asked to facilitate, conduct, or participate in training based on the materials it has developed.

The training materials must meet WCAG 2.0/2.1 (AA) success criteria to address the usability and accessibility needs of the people using the services, systems, applications and websites.

Training includes all activities related to developing and delivering training and educational materials and tools in support of projects for system development/deployments and production support (operations and maintenance). The contractor is responsible for developing and maintaining all training and user guides, frequently asked question (FAQs), release notes and training materials for KM developed and/or supported applications, including web and computer-based training (CBT). The contractor will, as needed, develop and provide training for requested systems, in person or through web-based and/or computer-based training tools.

Principal Tasks to be performed by the contractor shall include:
a. Developing and maintaining training processes and procedures
b. Developing training plans for KM-developed systems
c. Creating and updating user guides/training materials
d. Conducting annual review and updates of application user guides and training materials for KM systems
e. Creating/updating computer-based training

f. Developing materials and conducting classroom and web-based training
g. Researching and recommending training methods, tools, and technologies
h. Evaluating KM Helpdesk tickets to identify customer training needs;
i. Developing recommendations for measuring and tracking training effectiveness; and
j. Conducting survey/evaluation of training effectiveness.

6.3.9 **KM Helpdesk.** The KM Help Desk is a single call center supporting all KM customer requests for user support of all KM applications.

The contractor will be responsible for providing helpdesk and user support for applications and systems supported by KM. The contractor will be responsible for providing Tier I support by creating tickets and routing calls, as well as Tier II and Tier III support and escalations for troubleshooting known issues specific to KM supported applications. The contractor will be responsible for the use and management of the helpdesk tools such as the JIRA ticket tracking system.

The contractor will also be responsible for utilizing analysis of helpdesk trends both proactively and reactively. Reactive analysis includes the development of frequently asked questions and proposed system changes based on trends discovered in analysis of common user problems. Real-time analysis includes the live identification of potential system or network problems based on a spike in calls from users in a specific organization or of a specific system. The contractor will also be responsible for performing this analysis in real-time to ensure that issues in the production environment are uncovered and resolved quickly.

Principal Tasks to be performed by the contractor include operation, management and maintenance of the call center environment including Automated Call Distributor, Interactive Voice Response, and associated call center systems in addition to;
a. Providing Tier 1 Support including call screening and triage
b. Providing Tier 2 Support including issue resolution
c. Providing Tier 3 Support and escalation including subject matter expertise support
d. Management of trouble tickets
e. Maintaining the content of the knowledge repository/self-service portal
f. Providing help desk and customer standardized ad-hoc reporting
g. Establishing help desk metrics and monitoring and reporting as requested
h. Generating standardized reports every sprint
i. Providing proactive management of problem areas
j. Recording and report problems and resolution in the designated user support tracking system
k. Developing and supporting self-help capabilities
l. Developing lessons learned and utilize the lessons learned to aid in process improvements
m. Support IMS activations with extended service hours.

6.3.10 **Open Science**. In order for federal science to be reproducible, research outputs such as datasets, analytic code, and software need to well documented and shared with the public so that interested parties can test hypothesis and conclusions. This contract supports CDC scientist in the creation of open science packages with include scientific publication as well as the data and code that was used to develop the conclusions documented in the scientific work. This support entails working directly with CDC scientists as well as assisting with procedures for releasing and interlinking the components of an open science package. Based on requirements gathered, multiple KM systems will need to updated to meet future needs.

6.3.11 **Information Assurance (IA) Support.** The contractor IA Support team includes the activities necessary to ensure the security of KM applications and the adequacy of security controls meet all the

IT Security and Privacy Requirements for Federal systems, as defined by law, regulation, and HHS, DHS, CDC and OMB policy and guidance.

The contractor will be responsible for working directly with the KM Security Steward in the development of security plans, instructions, guidance, and operating procedures. The contractor will provide expertise throughout the application lifecycle and participates in security planning, risk assessments, drafting of IA policies and procedures, and development of security requirements.

The contractor will monitor and advise on IA-related requirements, mandates, Presidential Directives and regulations and ensures analysis, tests, and reviews are conducted in a timely manner. The contractor will also assist the KM Security Steward to develop Security Assessment and Authorization (SA&A) packages under the direction of the KM ISSO and reviews and evaluate the adequacy of security controls, including completing the Privacy Impact Assessment (PIA) document.

The contractor must have a proficient understanding and experience with the National Institute of Standards and Technology (NIST) Special Publications as well as cloud technologies such as, but not limited to, Azure and Amazon Web Services in order to evaluate vulnerabilities and risk in going through an accreditation for systems deployed and hosted at cloud service providers. KM is currently working with cloud providers with a FedRAMP certification, therefore the contractor must be familiar and have experience with performing a SA&A on systems hosted on a FedRAMP ATO.

Principal Tasks to be performed by the contractor shall include:

a. Assisting with the development of KM SA&A packages, including data and privacy documentation
b. Processing KM SA&A packages annual deliverables including Annual Assessments and Business Continuity Plans / Information System Contingency Plans at least 30 to 60 days before the due date
c. Coordinating and collaborating with the Cybersecurity Program Office (CSPO) as needed in support of the SA&A process, change management and ongoing continuous monitoring
d. Working with Project Teams on security requirements which includes attending project meetings, advising the Project Teams on the SA&A process and timelines, and collaborating to complete the required documentation to obtain an ATO or change request
e. Working with KM to implement IA activity efficiencies and process improvements including updating team SOPs and suggesting SA&A process improvements for internal team efficiency
f. Monitoring implementation of Corrective Action Plans (CAP), weakness management and Plans of Action and Milestones (POA&M)
g. Obtaining artifacts and drafting CAPs, POAM closures and assessing if the artifacts are sufficient to meet the control deficiency for POAM closure
h. Tracking SA&A deliverables and their due dates ensuring no deliverable is past due and Managing the document repository
i. Reporting to the KM Security Steward and ISSO on SA&A deliverables status
j. Performing proactive security analysis and testing of KM systems by self-reporting POAMs to CSPO if a deficiency is identified during the annual assessment or during the course of business;
k. Developing and conducting IA training by scheduling training sessions with Project Managers, developers and Business Analyst to ensure an understanding of the SA&A process and change management process;
l. Performing KM information security support activities including, but not limited to, vulnerability scans using Nessus, Web Inspect, Fortify and other tools as they become available; and
m. Integrating security with enterprise architecture (EA), and capital planning and investment control (CPIC) by completing stage-gate reviews for projects within TSB.

6.3.12 **Data Curation.**

To ensure that CDC science is easily discoverable proper document/data curation must occur. This requires document curation expertise that can guide the collection development plan for the CDC

repositories, provide original cataloging of documents with no current metadata record, and work with content creators to ingest new documents and ensure that they are acceptable for posting in an external repository. This includes support for the federal records storage and transfer project guided by the Strategic Business Initiatives Unit. This project is designed to import and store permanent and nonpermanent federal records into CDC Vault then transfer those records to the National Archives and Records Administration. Data curation requirements go beyond publication cataloging. Special expertise will be required to catalog scientific datasets as well as code. Assisting CDC staff members on the proper curation of their scientific output will also be required

6.3. 13 KNOWLEDGE MANAGEMENT IT PRODUCT DESIGN, DEVELOPMENT, ENHANCEMENT, AND OPERATION AND MAINTENANCE
(APPLICABLE TO ALL PERIODS)

6.3.13.1 **Document Operations and Clearance System (DOCS)**

DOCS has multiple subsystems, including eClearance, STARs, Data Use, Publishing Reporting, and TiPSTER. DOCS is currently undergoing a major system refresh. This includes a major software update, a system migration and a system architecture update are all occurring in concert. The contractor will be required to have staff that is capable of supporting this effort without significant delay or interruption of service. The DOCS subsystems are used by many organizations within CDC and serve as an important step in the communication between the CDC and the citizens of the United States.

eClearance, Data Use Agreements and STARs are currently built upon the Documentum/OpenText tech stack. It has been determined that this is no longer the best solution to support eClearance moving forward. A transition to a new backend is already underway. This new data driven backend will allow eClearance to be nimbler in adapting to new requirements in the future. It will also jettison unneeded code libraries that have to be maintained and can cause security issues.

The Data Use Agreement (DUA) portion of DOCS is currently supporting CDC's plan to standardize DUAs at CDC. This is an important initiative at CDC and will require new functionality to support requirements that come from the Immediate Office of the Director.

Publishing Reporting handles much of the statistics of KM, the measurement of the impact of KM systems and the impact and use of CDC publications as a whole. It is also providing impact reports to other federal stakeholders that are using the CPAP system environment. Publishing reporting mainly relies on API system calls to the other DOCS subsystems and CPAP to retrieve and process the statistical information.

Tipster is the supporting tools subsystem of DOCS based on JIRA. During the migration to AWS, Tipster will be doing a JIRA software refresh, going to the latest major software version. Since JIRA serves as a major component in the reporting and tracking of work done by and requested of the KM development and operations teams, the migration and upgrade will need to be done with little interference or impact.

1. Continue the transition away from Documentum/Open text to a data driven backend.
2. Update the business continuity plan and disaster recovery
3. Further develop DOCS APIs to work with CDC and non-CDC stake holders.
4. Meet with stakeholders and continue development and improvements to DOCS systems
5. Continue the development of the Data Use Agreement workflow and interface
6. Maintain and update Jira to keep the system in line with team needs
7. Expand eClearance to leverage AI to help improve document entry tasks and reduce user workload.
8. Expand eClearance to handle additional identities (Azure Entra ID, Login.gov)

9. Reclassify a portion of eClearance to support non-organizational users to have access to steps of the clearance process (external reviewers, external collaborative authors, etc),

6.3.13.2 **CDC Public Access Platform (CPAP)/ CDC Vault (CDCV)**

CPAP/CDCV utilize a common source code base with a configurable option for anonymous access (CPAP) or restricted access model (CDCV). They both heavily rely on Drupal, Islandora and SOLR and leverage both built-in and customized APIs to support the final product. In addition, CPAP has public APIs such as OAI-PMH and JSON that allows anyone in the public to retrieve the metadata catalog of the CPAP digital repository.

CPAP currently resides in an OCIO managed environment at AWS. Although OCIO is responsible for the images the contractor is responsible for all other maintenance. The contract will monitor an optimize the AWS cloud environments to ensure proper use of government funds.

CDCV This system is currently adding features to support becoming the official system to manage federal records for the CDC at large. As a part of this, development of the necessary APIs will be required to allow various CDC offices to interact with CDCV programmatically. Additionally, CDCV will be adding support to call NARA APIs to support the transition of and final disposition of federal records into the national archive.

6.3.13.3 **Data Discovery and Classification Tool (DDCT)**

The Data Discovery and Classification Tool (DDCT) is a tool that can help decision makers understand the nature and classification of their data. This tool has the ability to search through files and databases and provide a report of what sort of data is present. The tool can be used to identity PII, HIPPA, GDPR and/or PCI related data and provide examples from the dataset to the user to take appropriate action.

6.4 MANAGEMENT OBJECTIVES

- Allow the contractor maximum flexibility to innovatively manage program cost, schedule, performance, risks, warranties, contracts and subcontracts, vendors, and data required to deliver effective consulting services.
- Maintain clear government visibility into program cost, schedule, technical performance, and risk, including periodic reporting.
- Provide meaningful reporting and analytics that provide *CDC* with up-to-date and comprehensive information regarding technical and management performance.

6.5 ADMINISTRATIVE OBJECTIVES

- Utilize relevant tools and analysis techniques for analyzing, evaluating and presenting information gathered throughout the *[migration planning phases].* Describe approach and examples of relevant tools and analysis techniques for *[all relevant phases].*
- Provide *CDC* with decision making support in the form of relevant artifacts and work products.
- Describe in the proposal a set of performance metrics that will be used to monitor and assess performance of the KMTSS processes.

7 Deliverables:

All deliverables shall be submitted to the COR via email unless otherwise agreed upon. Unless otherwise specified, the Government will have a maximum of ten (10) working days from the day the deliverable is received to review the document, provide comments back to the contractor, and approve or disapprove the deliverable(s). The contractor will also have a maximum of ten (10) working days from the day comments are received to incorporate all changes and submit the final deliverable to the Government. All days identified in the deliverable table below are intended to be workdays unless otherwise specified.

All Task Order related reports shall be submitted to the Government via email. The contractor shall submit all required report(s)/deliverables in accordance with the following schedule: All reports shall reference and cite the contract number. Attachment IV provides the list of deliverables.

Item Description	Deliverable	Due Date	Deliver To
Contractor shall schedule a Kickoff meeting with the government for planning purposes within five (5) calendar days of this award.	Meeting minutes	Within five days after the meeting	One electronic copy to the COR
Contractor shall provide a monthly status report for each task utilizing Microsoft Word 2010 or newer version format for the document and emailed to the COR to include: *Monthly Status Report (MSR)* The MSR shall be prepared by the contractor and delivered to the CDC COR via email unless otherwise agreed upon. Each report shall be due on the fifteenth (15) of the calendar month. The MSR shall contain the following information: • Brief description of requirements. • Brief summary of accomplishments during the reporting period. • Deliverables submitted or progress on deliverable products. • Any current or anticipated problems and proposed solutions. • Brief summary of activity planned for the next reporting period. • Staffing Lists- The staffing list shall be by task number, with contractor employee name, labor category, managers name, physical location. Reports hall include vacancies and updates of new hires and departing staff.	Monthly task order status report	Submitted at time of invoice.	One electronic copy to the COR and the Contracting Officer.
Contractor shall provide a weekly financial report in an agreed to format and emailed to the COR and Gov't PM to include: • Financial spend across contract (all CLINs)	Weekly financial status report		One electronic to the COR and Gov't PM

• Financial report based upon activity/project • Financial report based upon activity/project with details on approved budget, actual spend and remaining budget projections • Financial performance trajectory including risk, issues and decisions needed by the government.			
Progress Meetings The Contractor shall attend progress meetings requested by the contracting activity or task order administration. The Contracting Officer, Contracting Officer's Representative (COR), and other Government personnel, as appropriate, may meet periodically with the Contractor to review the Contractor's performance. At these meetings the CO will apprise the Contractor of how the government views the Contractor's performance and the Contractor will apprise the Government of problems, if any, being experienced. Status updates of projects and deliverables will be provided. Appropriate action shall be taken to resolve outstanding issues. These meetings shall be at no additional cost to the government.	Ad Hoc reports	Quarterly timeframe.	One electronic copy to the COR
Quality Control Plan (QCP) A written document describing the internal staffing, procedures, and metrics the Contractor will use to meet the quality, quantity, timeliness, responsiveness, customer satisfaction, and other service delivery requirements for successful performance.	Initial QCP due with proposal. Follow-on QCP due no later than 30 business days following award to the KM COR and Contracting Officer. The KM COR and contractor will coordinate following the initial QCP to finalize appropriate metrics and any service level agreements (SLAs) for projects.	To be determine after award	One electronic copy to the COR

Quarterly In-Process Review (IPR) Presentation A MS PowerPoint briefing summarizing status, progress, recommendations and concerns in project and TO execution.	Submitted quarterly to the KM COR and KM designates. Presented quarterly to KM COR and leadership.	To be determine after award	One electronic copy to the COR
Transition-Out Results Report A written Report detailing the completion of transition activities and acknowledging successful completion of Transition and successfully transfer or knowledge, documentation, and GFE to the Government and any successor contractor.	Within 10 business days of the Government's request.	To be determine after award	One electronic copy to the COR

8 Performance Metrics:

Desired Outcomes	Required Services	Performance Standard	Acceptable Quality Level (AQL)	Monitoring Method (Quality Assurance Surveillance Plan/QASP)	Incentives/ Disincentives

Efficient and effective overall contract and project management	Contractor maintains high level of quality assurance, reliability, and completeness of tasks and projects.	Within cost, schedule, and properly staffed. Project- specific standards are established in the agreed-to Quality Control Plan.	At or below cost; work completed on-time or earlier; all staff meet CAOSS LCAT standards 100% of the time; QCP metrics are met	COR & Contracting Officer monitoring; deliverables; and reports	Favorable or unfavorable performance evaluation; allow option period to expire unexercised
Contract management and responsiveness	Responds to questions / concerns from COR and Contracting Officer within a reasonable time.	Response time is within a range of an hour up to one business day depending on the urgency and complexity.	100% of the time	COR & Contracting Officer monitoring and reports	Contractor will have to respond to the question / concern. Both positive and negative customer service will be reported into CPARS.
Invoices are accurate and timely	Accurate invoices are submitted in a timely manner.	No invoices within a 12-month period require suspension or disallowance due to mistakes, incompleteness or	95% of the time	Invoice; COR verification of accuracy	Contractor shall re-perform at own expense. Continued deficiency will be reported into CPARS.
The deliverables completed each month are accurate and clearly communicated.	See deliverables table.	High quality, fully edited, and accurate; delivered by due date.	95% of the time	Deliverable; COR verification of accuracy and quality	Contractor shall re-perform at own expense. Continued deficiency will be reported into CPARS.

9 Special Requirements:

9.1 TRAVEL

Local or international travel may be required to support the technology implementations. All travel is to be reimbursed only in accordance with the Federal Travel Regulations (FTRs) and Department of State Standardized Regulations (DSSR). The Contractor shall ensure that the requested travel costs will not exceed the amount authorized in this task order.

9.2 PERSONNEL

a) Certain skilled experienced professional and/or technical personnel are essential in order for this contract to be successful in performing the stated requirements. These personnel are defined as "Key Personnel" and are those persons whose resumes shall be submitted for approval or evaluation with the initial proposal. The key personnel shall not be removed from the contract work or replaced without compliance with paragraphs (b)

and (c) hereof.

b) If one or more of the key personnel for whatever reason becomes, or is expected to become, unavailable for work under this contract for a continuous period exceeding thirty (30) work days, or is expected to devote substantially less effort to the work than indicated in the proposal or initially anticipated, the contractor shall immediately notify the COR and shall, subject to the approval of the Contracting Officer, promptly provide a temporary or permanent replacement of such personnel with personnel of at least substantially equal ability and qualifications.

c) All requests for approval of substitutions hereunder must be in writing and provide a detailed explanation of the circumstances necessitating the proposed substitutions. They must contain a complete resume for the proposed substitute, and any other information requested by the Contracting Officer or needed by the COR to approve or disapprove the proposed substitution. The Contracting Officer or the COR will evaluate such requests and promptly notify the contractor of his approval or disapproval thereof in writing.

d) If the Contracting Officer determines that suitable and timely replacement of key personnel who have been reassigned, terminated or have otherwise become unavailable for the contract work is not reasonably forthcoming or that the resultant reduction of productive effort would be so substantial as to impair the successful completion of the contract or the services ordered, the contract may be terminated by the Contracting Officer for default or for the convenience of the Government, as appropriate, or, at the discretion of the Contracting Officer if he finds the contractor at fault for the condition, the contract price or fixed fee may be equitably adjusted downward to compensate the Government for any resultant delay, loss, or damage.

e) KM is willing to consider employees under the predecessor contract.

f) Key Personnel labor categories shall be proposed as identified or as an equivalent category with the corresponding experience, expertise, and certifications.

All contractor personnel shall be trained and skilled at the level necessary for execution of the Tasks as described in this performance work statement. No training cost will be reimbursed by the Government unless expressly requested by the Government and approved by the Contracting Officer

9.2.1 **Key Personnel.**

- CPAP/CDCV Application Engineer
- DOCS Application Engineer
- Data and Analytics Architect
- Systems Operations Engineer
- Quality Assurance Automations Engineer
- Library Sciences Data Curator

The Contractor shall propose, and provide Resumes for, the following Key Personnel.

CPAP/CDCV Application Engineer

This person shall be the primary developer of the CPAP and CDCV systems. This person will require a minimum of 10 years experience with Java, Eclipse, Drupal, SOLR and SOLR performance tuning, TOMCAT, Apache web server, PHP, Fedora Commons, Islandora, MySQL in order to support the existing codebase of CPAP/CDCV. They will need to have a detailed understanding of CDC secure coding practices and software development. They will need to understand PIV authentication with a focus on client certificate authentication of PIV tokens. In addition, they will need to have a solid understanding of the AWS operating environment and associated best practices with a eye towards leveraging Kubernetes and Docker. They will:

- Improve the overall functioning of KM software/solution delivery.
- Provide recommendations on new/improved software architecture, working within existing software and AWS virtual hardware components that optimize certain technology.
- Ensure KM customer business needs are met and exceeded.

- Skillfully extract information from clients to determine the project scope and design solutions.

DOCS Application Engineer

This person shall be the primary developer of the DOCS system and its subsystems. This person will require a minimum of 10 years experience with Java, Eclipse, Documentum 7.X, Opentext 16.X, SOLR and SOLR performance tuning, Tomcat, MS SQL, active directory authentication in order to support the existing system and the transition efforts of DOCS and the subsystems. They will need to have a detailed understanding of CDC secure coding practices and software development. In addition, they will need to have a solid understanding of the AWS operating environment and associated best practices with a eye towards leveraging Kubernetes and Docker. They will:

- Improve the overall functioning of KM software/solution delivery.
- Provide recommendations on new/improved software architecture, working within existing software and AWS virtual hardware components that optimize certain technology.
- Ensure KM customer business needs are met and exceeded.
- Skillfully extract information from clients to determine the project scope and design solutions.

Data and Analytics Architect

This person shall be the primary database architect for all KM systems. This person will require a minimum 10 years experience with Microsoft SQL with a focus on 2016-2019 server, SQL server high availability functions with an emphasis on database mirroring, SQL CLR, MySQL, Kubernetes, Docker, Red-Gate SQL Monitor, Visual Studio, Python, Database Security, encrypted data elements / columns / tables, database performance monitoring and troubleshooting, database tuning and optimization, external data updates using API calls and batch loads, SQL server R development, SSIS development, Microsoft Power Shell, ERStudio database modeling, Visio. They will need to have a detailed understanding of CDC secure coding practices and software development. In addition, they will need to have a solid understanding of the AWS operating environment and associated best practices. They will:

- Improve the overall functioning of KM database software/solution delivery.
- Provide recommendations on new/improved software architecture, working within existing software and AWS virtual hardware components that optimize certain technology.
- Ensure KM customer business needs are met and exceeded.
- Skillfully extract information from clients to determine the project scope and design solutions.

Systems Operations Engineer

This person(s) will be the core of the KM operations effort. This person(s) will require a minimum of 5 years experience with Microsoft Server (2012, 2016, 2019), IIS, Apache Web Server, Apache Tomcat, Chef Automate, Kubernetes, Docker, Splunk, PRTG, AWS instances / VPCs / VPNs / routing, DNS, Certificates, PIV authentication, They will manage all of the servers / instances / containers, They will be the primary person(s) working to maintain, migrate and troubleshoot all of the KM systems infrastructure. They will need to have a detailed understanding of CDC secure systems deployment and have a history of working with external teams to achieve objectives. They will need to have a solid understanding of AWS products and services.

- Maintain and improve the overall functioning of the KM operating environment
- Provide recommendations on new/improved AWS service options
- Improve KM server management practices and automation scripts/tasks
- Skillfully work with external partners to achieve deployment and maintenance goals and objectives
- Ensure KM customer business needs are met and exceeded

9.3 EQUIPMENT AND INFORMATION:

(a) Government-Furnished Property (GFP). In accordance with the terms of FAR 52.245-1, Government Property, the Government reserves the right to supply the Contractor, as Government-furnished property, any additional supplies, equipment, and materials determined by the Contracting Officer to be necessary and in the best interest of the Government.
(b) Contractor-Acquired Property (CAP). The Contractor must receive written consent from the Contracting Officer prior to purchase of any CAP not expressly identified in the contract, and as defined in FAR 52.245-1.
(c) Accountable and Sensitive Government Property. The Government will provide property labels and other identification for contractor-acquired Government property that is considered Accountable as defined in the HHS Logistics Management Manual (LMM) (http://www.hhs.gov/hhsmanuals/logisticsmanual/LMM.pdf) or considered Sensitive as defined in CDC's Sensitive Items List http://pgo.cdc.gov/pgo/webcache/content/DocsRepository/Logistics/REVISED_SENSITVE_ITEM_10042010.xlsx
(d) The contractor shall be responsible for the control and accountable record keeping of any Government property used in the performance of this contract predominately outside the confines of a Government controlled workspace in accordance with HHS LMM Appendix Q, HHS Contracting Guide for Contract of Government Property http://www.hhs.gov/hhsmanuals/logisticsmanual/Appendix%20Q_HHS%20Contracting%20Guide.pdf
(e) The Chief of the Logistics Management Branch, PGO, Centers for Disease Control and Prevention (CDC), is hereby designated as the Property Administrator for this contract. The Contractor shall identify each item of equipment furnished by the Government to the Contractor or acquired by the Contractor using contract funds, with a suitable decal, tag, or other marking, as prescribed by the Property Administrator, and shall follow the guidance set forth in Appendix Q, HHS Contracting Guide for Contract of Government Property http://www.hhs.gov/hhsmanuals/logisticsmanual/Appendix%20Q_HHS%20Contracting%20Guide.pdf

9.4 STANDARD FOR SECURITY CONFIGURATIONS:

The Contractor shall apply approved security configurations to information technology (IT) that is used to process information on behalf of HHS. The Contractor will meet requirements in Section 4 of this PWS and will comply with CDC security requirements for logical and physical access to CDC IT systems, facilities, and workspaces that apply to all CDC employees and non-employees.

9.5 ACCESS REQUIREMENTS:

The Contractor shall comply with agency personal identity verification procedures identified in the contract that implement Homeland Security Presidential Directive-12 (HSPD-12), Office of Management and Budget (OMB) guidance M-05-24 and Federal Information Processing Standards Publication (FIPS PUB) Number 201.

During the period of this contract, the rights of ingress and egress to and from any office for Contractor's personnel shall be made available as deemed necessary by the Government. All Contractor employees, whose duties under this contract require their presence at any Government facility, shall be clearly identifiable by a distinctive badge furnished by the Government. All prescribed information shall immediately be delivered to the appropriate Government Security Office for cancellation or disposition upon the termination of employment of any Contractor personnel. All on-site Contractor personnel shall abide by security regulations applicable to that site.

The Contractor shall insert this clause in all subcontracts when the subcontractor is required to have routine physical access to a Federally controlled facility and/or routine access to a Federally controlled information system.

9.6 ADDITIONAL CLAUSES AND PROVISIONS

A. Baseline Security Requirements

1) **Applicability.** The requirements herein apply whether the entire contract or order (hereafter "contract"), or portion thereof, includes either or both of the following:

   a. Access (Physical or Logical) to Government Information: A Contractor (and/or any subcontractor) employee will have or will be given the ability to have, routine physical (entry) or logical (electronic) access to government information.

   b. Operate a Federal System Containing Information: A Contractor (and/or any subcontractor) employee will operate a federal system and information technology containing data that supports the HHS mission. In addition to the Federal Acquisition Regulation (FAR) Subpart 2.1 definition of "information technology" (IT), the term as used in this section includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources.

2) **Safeguarding Information and Information Systems.** In accordance with the Federal Information Processing Standards Publication (FIPS)199, *Standards for Security Categorization of Federal Information and Information Systems*, the Contractor (and/or any subcontractor) shall:

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

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

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

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

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

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

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

[ ] No PII [X] Yes PII

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

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

5) **Controlled Unclassified Information (CUI).** CUI is defined as "information that laws, regulations, or Government-wide policies require to have safeguarding or dissemination controls, excluding classified information." The Contractor (and/or any subcontractor) must comply with *Executive Order 13556, Controlled Unclassified Information, (implemented at 3 CFR,* part 2002*)* when handling CUI. 32 C.F.R. 2002.4(aa) As implemented the term "h*andling"* refers to "…any use of CUI, including but not limited to marking, safeguarding, transporting, disseminating, re-using, and disposing of the information." 81 Fed. Reg. 63323. All sensitive information that has been identified as CUI by a regulation or statute, handled by this solicitation/contract, shall be:

   a. marked appropriately;

   b. disclosed to authorized personnel on a Need-To-Know basis;

   c. protected in accordance with NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* applicable baseline if handled by a Contractor system operated on behalf of the agency, or NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations* if handled by internal Contractor system; and

   d. returned to HHS control, destroyed when no longer needed, or held until otherwise directed. Destruction of information and/or data shall be accomplished in accordance with NIST SP 800-88*, Guidelines for Media Sanitization*.

6) **Protection of Sensitive Information**. For security purposes, information is *or* may be sensitive because it requires security to protect its confidentiality, integrity, and/or availability. The Contractor (and/or any subcontractor) shall protect all government information that is or may be sensitive in accordance with OMB Memorandum M-06-16, *Protection of Sensitive Agency Information* by securing it with a FIPS 140-2 validated solution.

7) **Confidentiality and Nondisclosure of Information**. Any information provided to the contractor (and/or any subcontractor) by HHS or collected by the contractor on behalf of HHS shall be used only for the purpose of carrying out the provisions of this contract and shall not be disclosed or made known in any manner to any persons except as may be necessary in the performance of the contract. The Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its employees and subcontractors shall be under the supervision of the Contractor. Each Contractor employee or any of its subcontractors to whom any HHS records may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such employee or subcontractor can be used only for that purpose and to the extent authorized herein.

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

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

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

9) **Government Websites.** All new and existing public-facing government websites must be securely configured with Hypertext Transfer Protocol Secure (HTTPS) using the most recent version of Transport Layer Security (TLS). In addition, HTTPS shall enable HTTP Strict Transport Security (HSTS) to instruct compliant browsers to assume HTTPS at all times to reduce the number of insecure redirects and protect against attacks that attempt to downgrade connections to plain HTTP. For internal-facing websites, the HTTPS is not required, but it is highly recommended.

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

*See **Appendix D** for baseline deliverables.*

11) **Standard for Encryption.** The Contractor (and/or any subcontractor) shall:

a. Comply with the *HHS Standard for Encryption of Computing Devices and Information* to prevent unauthorized access to government information.

b. Encrypt all sensitive federal data and information (i.e., PII, protected health information [PHI], proprietary information, etc.) in transit (i.e., email, network connections, etc.) and at rest (i.e., servers, storage devices, mobile devices, backup media, etc.) with FIPS 140-2 validated encryption solution.

c. Secure all devices (i.e.: desktops, laptops, mobile devices, etc.) that store and process government information and ensure devices meet HHS and CDC-specific encryption standard requirements. Maintain a complete and current inventory of all laptop computers, desktop computers, and other mobile devices and portable media that store or process sensitive government information (including PII).

d. Verify that the encryption solutions in use have been validated under the Cryptographic Module Validation Program to confirm compliance with FIPS 140-2. The Contractor shall provide a written copy of the validation documentation to the COR *[CDC-provided delivery date]*.

e. Use the Key Management system on the HHS personal identification verification (PIV) card or establish and use a key recovery mechanism to ensure the ability for authorized personnel to encrypt/decrypt information and recover encryption keys. Encryption keys shall be provided to CDC Office of Chief Information Security Officer (OCISO).

12) **Contractor Non-Disclosure Agreement (NDA)**. Each Contractor (and/or any subcontractor) employee having access to non-public government information under this contract shall complete the CDC non-disclosure agreement, as applicable. A copy of each signed and witnessed NDA shall be submitted to the Contracting Officer (CO) and/or CO Representative (COR) prior to performing any work under this acquisition.

See Appendix C for the HHS Contractor Non-Disclosure Agreement.

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

    a. The Contractor shall assist the CDC SOP or designee in reviewing the PIA at least every three years throughout the system development lifecycle (SDLC)/information lifecycle, or when determined by the CDC SOP that a review is required based on a major change to the system (e.g., new uses of information collected, changes to the way information is shared or disclosed and for what purpose, or when new types of PII are collected that could introduce new or increased privacy risks), whichever comes first.

B. Training

1) **Mandatory Training for All Contractor Staff.** All Contractor (and/or any subcontractor) employees assigned to work on this contract shall complete the applicable HHS/CDC Contractor Information Security Awareness, Privacy, and Records Management training (provided upon contract award) before performing any work under this contract. Thereafter, the employees shall complete *CDC Security Awareness Training (SAT)* and Records Management training at least ***annually***, during the life of this contract. All provided training shall be compliant with HHS training policies.

2) **Role-Based Training.** All Contractor (and/or any subcontractor) employees with significant security responsibilities (as determined by the program manager) must complete Role-Based training (RBT) ***within 60 days*** of assuming their new responsibilities. Thereafter, they shall complete RBT at least ***annually*** in accordance with HHS policy and the *HHS Role-Based Training (RBT) of Personnel with Significant Security Responsibilities Memorandum*.

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

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

C. Rules of Behavior

1) The Contractor (and/or any subcontractor) shall ensure that all employees performing on the contract comply with the *HHS Information Technology General Rules of Behavior.*

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

D. Incident Response

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

A privacy Job is a type of incident and is defined by Federal Information Security Modernization Act (FISMA) as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose.
OMB Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information" (03 January 2017) states:

> **Definition of an Incident:**
> *An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.*
>
> **Definition** of a **Breach:**
> *The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for another than authorized purpose.*

It further adds:

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

The HHS *Policy for IT Security and Privacy Incident Reporting and Response* further defines a breach as "a suspected or confirmed incident involving PII" .

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

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

2) All contractors and subcontractors shall properly encrypt PII in accordance with OMB Circular A-130 and other applicable policies, including CDC-specific policies, and comply with HHS-specific policies for protecting PII. To this end, all contractors and subcontractors shall protect all sensitive information, including any PII created, stored, or transmitted in the performance of this contract so as to avoid a secondary sensitive information incident with FIPS 140-2 validated encryption.

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

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

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

to access Federal information, and identify the initial attack vector.

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

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

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

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

E. Position Sensitivity Designations

All Contractor (and/or any subcontractor) employees must obtain a background investigation commensurate with their position sensitivity designation that complies with Parts 1400 and 731 of Title 5, Code of Federal Regulations (CFR).

Level 1 : Non-sensitive

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

F. Homeland Security Presidential Directive (HSPD)-12

The Contractor (and/or any subcontractor) and its employees shall comply with Homeland Security Presidential Directive (HSPD)-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*; OMB M-05-24; FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*; HHS HSPD-12 policy; and *Executive Order 13467, Part 1 §1.2.*

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

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

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

G. Contract Initiation and Expiration

1) **General Security Requirements.** The Contractor (and/or any subcontractor) shall comply with

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

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

2) **System Documentation.** Contractors (and/or any subcontractors) must follow and adhere to NIST SP 800-64, *Security Considerations in the System Development Life Cycle*, at a minimum, for system development and provide system documentation at designated intervals (specifically, at the expiration of the contract) within the EPLC that require artifact review and approval.

3) **Sanitization of Government Files and Information.** As part of contract closeout and at expiration of the contract, the Contractor (and/or any subcontractor) shall provide all required documentation to the CO and/or COR to certify that, at the government's direction, all electronic and paper records are appropriately disposed of and all devices and media are sanitized in accordance with NIST SP 800-88, *Guidelines for Media Sanitization*.

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

5) **Contractor Responsibilities Upon Physical Completion of the Contract**. The contractor (and/or any subcontractors) shall return all government information and IT resources (i.e., government information in non-government-owned systems, media, and backup systems) acquired during the term of this contract to the CO and/or COR. Additionally, the Contractor shall provide a certification that all government information has been properly sanitized and purged from Contractor-owned systems, including backup systems and media used during contract performance, in accordance with HHS and/or *CDC* policies.

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

H. Records Management and Retention

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

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

Section 508 and Accessibility Requirements

Part A – Provision
Reference HHSAR 352.239-73[8] Electronic Information and [Communication] Technology Accessibility Notice. [(Deviation)]
[(a) Any offeror responding to this solicitation must comply with established HHS Information and Communication Technology (ICT) accessibility standards. Information about Section 508 is available at https://www.hhs.gov/web/section-508/index.html.
(b) The Section 508 accessibility standards applicable to this solicitation are stated in the clause at 352.239-79 Information and Communication Technology Accessibility. In order to facilitate the Government's determination whether proposed ICT supplies, products, platforms, information, and documentation meet applicable Section 508 accessibility standards, offerors must submit an appropriate HHS Section 508 Accessibility Conformance Checklist

(see https://www.hhs.gov/web/section-508/accessibility-checklists/index.html) or an Accessibility Conformance Report (ACR) (based on the Voluntary Product Accessibility Template (VPAT) see https://www.itic.org/policy/accessibility/vpat), in accordance with the completion instructions. The purpose of the checklists and conformance reports are to assist HHS acquisition and program officials in determining whether proposed ICT supplies, products, platforms, information, and documentation conform to applicable Section 508 accessibility standards. Checklists and ACRs evaluate—in detail—whether the ICT conforms to specific Section 508 accessibility standards and identifies remediation efforts needed to address conformance issues.
(c) If an offeror claims its supplies or services meet applicable Section 508 accessibility standards, and it is later determined by the Government, i.e., after award of a contract or order, that supplies, products, platforms, information, documentation, or services support delivered do not conform to the described accessibility standards, remediation of the supplies, products, platforms, information, documentation, or services support to the level of conformance specified in the contract will be the responsibility of the Contractor at its expense.
(d) In order to facilitate the Government's determination whether proposed ICT supplies meet applicable Section 508 accessibility standards, offerors must submit an Accessibility Conformance Report, in accordance with its completion instructions and tailored to the requirements in the solicitation. The purpose of the Report is to assist HHS acquisition and program officials in determining whether proposed ICT supplies conform to applicable Section 508 accessibility standards. The template allows offerors or developers to self-evaluate their supplies and document, in detail, whether they conform to a specific Section 508 accessibility standard, and any underway remediation efforts addressing conformance issues. Instructions for preparing the Template are available at https://www.section508.gov/.
(e) Additionally, offerors must provide enough information to assist the Government in determining that the ICT services conform to Section 508 accessibility standards, including any underway remediation efforts addressing conformance issues.
(f) Respondents to this solicitation must identify any inability to conform to Section 508 requirements. If an offeror claims its supplies or services meet applicable Section 508 accessibility standards, and it is later determined by the Government, i.e., after award of a contract or order, that supplies or services delivered do not conform to the described accessibility standards, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its expense.
(g) Items delivered as electronic content must be accessible to HHS acceptance criteria. Checklist for various formats are available at http://508.hhs.gov/. Materials, other than items incidental to contract management, that are final items for delivery should be accompanied by the appropriate checklist, except upon approval of the Contracting Officer or Contracting Officer's Representative.

Part B - Clause
352.239-74[9] Electronic, Information, and Communication Technology Accessibility.
[(Deviation)]
(a) Pursuant to Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998, all information and communication technology (ICT) supplies, products, platforms, information, documentation, and services, or support developed, acquired, maintained or delivered under this contract or order must comply with the Revised 508 Standards, which are located at 36 C.F.R. 1194.1 and Appendices A, B, and C, and are available at https://www.access-board.gov/ict/. Information about Section 508 is available at https://www.hhs.gov/web/section-508/index.html.
(b) Additional Section 508 accessibility standards applicable to this contract or order are identified as follows:
205 WCAG 2.0 Level A & AA Success Criteria
302 Functional Performance Criteria
502 Inoperability with Assistive Technology
503 Applications
504 Authoring Tools
602 Support Documentation
603 Support Services
If it is determined by the Government that ICT supplies, products, platforms, information, documentation, and services support provided by the Contractor do not conform to the described accessibility standards in the contract, remediation of the supplies, products, platforms, information, documentation, or services support to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.
(c) In the event of a modification(s) to this contract or order, which adds new ICT supplies or services or revises the

type of, or specifications for, supplies, products, platforms, information, documentation, or services support, the Contracting Officer shall require that the Contractor submit a completed HHS Section 508 Accessibility Conformance Checklist (see https://www.hhs.gov/web/section-508/accessibility-checklists/index.html) or an Accessibility Conformance Report (ACR) (based on the Voluntary Product Accessibility Template (VPAT) see https://www.itic.org/policy/accessibility/vpat), and any other additional information necessary to assist the Government in determining that the ICT supplies or services conform to Section 508 accessibility standards. If it is determined by the Government that ICT supplies, products, platforms, information, documentation, and services support provided by the Contractor do not conform to the described accessibility standards in the contract, remediation of the supplies, products, platforms, information, documentation, or services support to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

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

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