Department of Health and Human Services (DHHS)

Administration for Strategic Preparedness and Response (ASPR)

Office of Emergency Management (OEM) and Medical Operations

Medical Reserve Corps (MRC)

**PERFORMANCE WORK STATEMENT (PWS)**

Agile Software Development for Website Services

**9 February 2023**

**1.0 BACKGROUND:**

Under this Blank Purchase Agreement (BPA) call, the contractor shall provide services that can affect positive and timely change and drive “process and website services delivery improvements” across the Medical Reserve Corps.

The website redesign began in calendar year 2020 achieved Minimum Viable Product (MVP) milestone in July 2021. The Medical Reserve Corps senior leadership anticipates that an additional 18-24 months after the first BPA call award will be necessary to achieve the “fully operational” project milestone.

On premises cloud hosting is provided by the ASPR Information Technology Services Division (ITSD), Enterprise Management Branch (EMB).

**2.0** **PURPOSE AND SCOPE**:

The scope of work under this BPA call is to provide federal website design and development services as defined in “Tasks” section 4.0 below in support of the public health emergency response missions of ASPR, including but not limited to the Medical Reserve Corps.

**3.0** **APPLICABLE DOCUMENTS**

 3.1 ASPR Strategic Plan 2022 – 2026 <https://aspr.hhs.gov/stratplan/Pages/default.aspx>

 3.2 Pandemic and All-Hazards Preparedness and Advancing Innovation Act of 2019

 3.3 *Security and Privacy Language for Information and Information Technology Procurements*, 3 March 2021, version 3.2

**4.0 DESCRIPTION OF SERVICES/TASKS:**

TASK 4.1 Technical Kick-Off Meeting

The contractor shall participate and prepare briefing materials for a Technical Kick-Off Meeting to be held no later than ten (10) business days after BPA call award.

The Federal Program Manager (Agile Product Owner) will collaborate with the contractor team at the technical kick-off meeting to discuss and establish total user story points and open-source software development priorities and any technical debt incurred for this BPA call. Development priorities illustrative of the Sprint Backlog include user stories for enhancement of the “unit registration”.

TASK 4.2 WEBSITE APPLICATION OPERATION AND MAINTENANCE SERVICES

The Contractor shall provide the labor, materials, and supervision required to maintain the MRC website open-source software applications and associated components, including legacy, open-source software.

The Government provides on-premises cloud hosting infrastructure for the MRC website.

* The contractor shall provide technical support for all MRC website applications.
* The contractor shall provide holistic lifecycle sustainment for the operations, maintenance, and enhancement of website applications.
* The Contractor shall work cooperatively with federal personnel to identify and resolve Help Desk tickets within the timeframe established by the MRC Web Project Manager.
* The contractor shall resolve functional defects and change requests for MRC website applications. The Federal PM must approve all change request in writing in advance.
* The contractor shall update all relevant documentation and archive documents on a repository to be designated by the MRC Web Project Manager. Documentation includes but is not limited to open-source software development, user training documentation, website performance analytics, asset inventory, configuration management, software release notes, governance/compliance, and system documentation. The contractor shall update the System Design Document (SSD) within 15 business days after each major, open-source software release.

TASK 4.3. WEBSITE DEVELOPMENT, MODERNIZATION, AND ENHANCEMENT (DME)

The contractor shall further develop, modernize, and enhance the website open-source software using Agile project methodologies such as but not limited to SCRUM, Extreme Programming, Scaled Agile Framework (SAFe), Kanban, etc.

Commercial-off-the-shelf software is permissible provided that is compatible with the “as built” open-source website architecture and has mimimal modification to the ASPR enterprise environment.

DME includes all phases of total lifecycle development including but not limited to requirements gathering and analysis, design, build, testing deployment and maintenance, and related artifacts and technical and user training documentation.

The contractor shall complete releases of working software on a regularly schedule basis.

The contractor shall ensure that all software developed under this BPA call is compatible with the federal enterprise architecture, observe secure coding and best practices.

TASK 4.4. Training Support

The contractor shall provide training materials and conduct training for the website applications.

TASK 4.5. REPORT DEVELOPMENT

The Contractor shall create and maintain reports to be used internally, appropriate metrics to enable data driven decision making. At every stage of a project, the contractor shall measure how well our service is working for our users. This includes measuring how well a system performs and how people are interacting with it in real-time for business management purposes, as well as other business purposes.

TASK 4.6. MONTHLY REPORT AND INVOICING

The contractor shall report contract progress on milestones, deliverables, and problem resolution and meet with the Contracting Officer’s Representative virtually no less than bi-weekly in a meeting to be held remotely by Microsoft Teams. The contractor shall update the risk register at each bi-weekly contract progress meeting to pro-actively mitigate risks to contract performance.

The contractor shall submit a Monthly Report and invoice monthly no later than the 10th day of the month following the prior period of performance. Each Monthly Report shall contain contract line-item information on problem resolution, risk management, cost burndown, labor hours and materials expended to date.

TASK 4.7 GOVERNANCE

The contractor shall achieve and maintain full compliance with the HHS OCIO Enterprise Performance Life Cycle (EPLC) and comply with OCIO regulations and authorities pertaining to the performance of all activities under this BPA call.

The contractor shall report breaches of security and privacy in a timely manner using Incident Response protocols established by the OCIO Information Systems Security Officer (ISSO). The Medical Reserve Corps (MRC) website is classified for authorization to operate (ATO) purposes under the ASPR Web Enterprise ATO.

5.0 TRANSITION OUT

The contractor shall provide all labor, materials, and supervision for the orderly transition in and out of the BPA Call.

The contractor shall provide a transition plan with milestones, deliverables, roles and responsibilities, and risk management

6. 0 CONTRACTOR PERSONNEL

The Contractor shall provide qualified personnel to perform all requirements specified in the BPA call Performance Work Statement (PWS).

 6.1 Key Personnel:

The Contractor shall provide a Web Project Manager who shall be responsible for all Contractor work performed under each BPA Call. The Web Project Manager shall be a single point of contact for the Contracting Officer and the COR. It is anticipated that the Web Project Manager shall be one of the senior level employees provided by the Contractor for these work efforts.

The name of the Web Project Manager, and the name(s) of any alternate(s) who shall act for the Contractor in the absence of the Web Project Manager, shall be provided to the Government as part of the Contractor's proposal. The Web Project Manager is further designated as *Key* by the Government.

During any absence of the Web Project Manager, only one alternate shall have full authority to act for the Contractor on all matters relating to work performed under this contract. The Web Project Manager and all designated alternates shall be able to read, write, speak, and understand English. Additionally, the Contractor shall not replace the Web Project Manager without prior approval from the Contracting Officer.

The Web Project Manager shall be available to the COR via telephone between the hours of 8:00 a.m. to 5:00 p.m. EST, Monday through Friday, and shall respond to a request for discussion or resolution of technical problems within 24 hours of notification.

Key Personnel – Web Project Manager (WPM): At a minimum, submit a resume for the proposed BPA Web Project Manager. It is desired that Quoters proposed a Web Project Manager that is certified by the Project Management Institute (PMI) as Project Management Professionals (PMP) with a minimum of seven years of experience with performing same or similar tasks described in the PWS.

 6.2 Key Personnel Positions for this BPA call

 Web Project Manager - III

 Web Software Developer (Full Stack Developer) – II

6.3 Replacement of Key Personnel:

Before replacing any individual designated as *Key* by the Government, the Contractor shall notify the Contracting Officer no less than 15 business days in advance, submit written justification for replacement, and provide the name and qualifications of any proposed substitute(s). All proposed substitutes shall possess qualifications equal to or superior to those of the *Key* person being replaced, unless otherwise approved by the Contracting Officer. The Contractor shall not replace *Key* Contractor personnel without approval from the Contracting Officer. *Key* personnel will be outlined for each requirement in the respective BPA Calls. Note: The Government may designate additional Contractor personnel as *Key* at the time of award.

Contractor *Key* personnel shall not be assigned by the Contractor to more than one key position for this requirement, unless authorized in individual BPA Calls by the Contracting Officer or the COR.

**6.0 DELIVERABLES**

| **Deliverable** | **Frequency** | **# Of Copies**  | **Medium/Format** | **Submit to** |
| --- | --- | --- | --- | --- |
| Technical Kick-Off Meeting(Federal PM & Contractor Web Project Manager leads this technically focused meeting)(Estimated 90 min.) | No later than 15 business days after BPA call award date. |  1 | PDF/Email/MS Word (.doc/.docx)/MS Excel (.xls/.xlsx) |  C.O., PM |
| Project Plan | No later than 15 business days after the technical kickoff meeting | 1 | PDF/Email/MS Word (.doc/.docx)/MS Excel (.xls/.xlsx) | COR, CO, PM |
| Invoices/Monthly Report/Risk Register/Cost Burndown | No later than the 10th of the month after the prior monthly period of performance is closed out  | 1 | PDF/Email/MS Word (.doc/.docx)/MS Excel (.xls/.xlsx) | COR, C.O. |
| Test Plan | One per release. Delivery date is dependent on project plan | 1 | PDF/Email/MS Word (.doc/.docx)/MS Excel (.xls/.xlsx) | COR, Federal PM |
| Release Readiness Briefing  | Upon completion of User Acceptance Testing (UAT) for each release of working software. | 1 | PDF/Email/MS Word (.doc/.docx)/MS Excel (.xls/.xlsx) | COR, Federal PM |
| System Design Document | Update within 15 business days after each release of working software |  1 | PDF/Email/MS Word (.doc/.docx)/MS Excel (.xls/.xlsx) | COR, Federal PM |
| Report Development | Per report, see Task 4.5 for types of reports |  1 | PDF/Email/MS Word (.doc/.docx)/MS Excel (.xls/.xlsx) | COR, CO, PM |

**7.0 ACCEPTANCE CRITERIA FOR DELIVERABLES:**

During the review of deliverables, the designated COR shall have the right to reject or require correction of any deficiencies found in the deliverables. In the event of rejection of any deliverable, the Contractor will be notified in writing by the COR of the specific reasons why the deliverable is being rejected. The Contractor shall correct the rejected deliverable and return it to the appropriate COR. The following list of acceptance criteria applies to all task:

1. Completeness, clarity, timeliness, organization, consistency, meets requirements, quality, grammatically correct, technical accuracy, and meet Agency Standards for documentation.
2. Where appropriate, deliverables shall also be evaluated for adherence to and enterprise-wide processes.
3. All deliverables shall demonstrate quality assurance and control aspects of each task.
4. Additional acceptance criteria may be specified in individual work requests.

**8.0 PERIOD OF PERFORMANCE**

This BPA Call shall consist of a Base Period and 3 one-year option period.

|  |  |
| --- | --- |
| **BPA Period** | **Ordering Period** |
| Option Period One (I) | 12 months |
| Option Period Two (II) | 12 months |
| Option Period Three (III) | 12 months |
| Option Period Four (IV) | 12 months |

**9.0 PLACE OF PERFORMANCE, WORK HOURS AND SCHEDULE**

The place of performance is offsite at the contractor’s facility or remotely via telework.

The contractor shall provide coverage during the core hours of 8:00 a.m. through 5:00 p.m. eastern, Monday through Friday.

## 10.0 GOVERNMENT FURNISHED PROPERTY (GFP)

The Government anticipates that the planned information technology GFP (material, equipment, and/or information) may be provided to support collaboration efforts in the performance of the task orders. This information is provided for informational purposes only.

|  |  |
| --- | --- |
| Contractor Personal Identification Verification (PIV) Badge (Dependency: PIV badge must be issued prior to issuance of any government issued laptop computer) | Per person requiring regular access to OCIO network resources and/or physical facility |
| ASPR ITSD Issued Laptop with Virtual Personal Network Access.  | Per person requiring access to OCIO network |

## 11.0 GOVERNMENT FURNISHED INFORMATION (GFI)

All documents related to earlier releases are contained in the MRC Website Redesign project folder and will be available to the Contractor during performance.

ASPR Cybersecurity Risk Management System is limited to selected management level contractor personnel, i.e., Web Project Manager.

SPRINT Backlog and User Story log located on the ASPR ITSD Microsoft Azure DevSecOps on-premises cloud infrastructure.

System Design Document (SSD) current version will be provided upon BPA Call award.

**12.0 MANDATORY TRAINING FOR CONTRACTORS**

 **12.1** All contractor personnel who are issued personal identity verification (PIV) badges or perimeter badges must complete the following training before working unescorted (Training shall be coordinated with the COR). The Government will provide the required training listed below regardless of duty location, or or offsite.

* + - Annual Privacy Awareness Training (approx. 45 minutes).
		- Records Management Employees & Contractors (approx. 45 minutes).
		- Annual Cybersecurity Training (approx. 45 minutes).

 **12.2** All contractor personnel shall possess and maintain current certifications and training, required by OSHA, Department of Transportation (DOT), Department of the Treasury, trade unions, and any other applicable bodies, related to their duties at ASPR.

 **12.3** All contractor personnel shall be required to sign a Non-Disclosure Agreement (NDA) prior to being granted access to the HHS network. A background check will be performed on contractor personnel after BPA call award.

**13.0 FACILITIES:** The Government will provide limited access to the government's facilities, as specified below:

Administration for Strategic Preparedness & Response (ASPR)

Thomas P. O’Neill Office Building (moving to Constitution Ave., the date is TBD)

200 C. Street SW

Washington DC 20024

 **14.0** **QUALITY CONTROL:**  Quality Control is the responsibility of the contractor.

14.1 The contractor is responsible for the delivery of quality services to the Government.

The Contractor shall develop, implement, and maintain an effective Quality Control System which includes a written Quality Control Plan (QCP). The QCP shall implement standardized procedure/methodology for monitoring and documenting contract performance to ensure all contract requirements are met.

The Contractors’ QCP must contain a systematic approach to monitor operations to ensure acceptable services/products are provided to the Government. The QCP, as a minimum, shall address continuous process improvement; procedures for scheduling, conducting and documentation of inspection; discrepancy identification and correction; corrective action procedures to include procedures for addressing Government discovered non-conformances; procedures for root cause analysis to identify the root cause and root cause corrective action to prevent re-occurrence of discrepancies; procedures for trend analysis; procedures for collecting and addressing customer feedback/complaints.

The contractor shall upon request provide to the Government their quality control documentation. After acceptance of the quality control plan the contractor shall receive the Contracting Officer’s acceptance in writing of any proposed change to their QC system.

14.2 Quality Assurance: The government shall evaluate the contractor’s performance under this contract in accordance with the Governments Quality Assurance Surveillance Plan.

**15.0 OBSERVANCE of Legal Holidays and Administrative Leave**

For work to be performed at Government site(s), the Contractor shall establish a standard holiday schedule that coincides exactly with the Government's schedule for employees working on a Government site. Holidays observed are listed below. For Government site work, holidays and other non-workdays are not billable unless work is specifically requested by the Government and productive hours are performed on those days. The following is a list of the official Federal Government holidays:

(1) New Year's Day (7) Labor Day

(2) Martin Luther King's Birthday (8) Columbus Day

(3) President’s Day (9) Veterans Day

(4) Memorial Day (10) Thanksgiving Day

(5) Juneteenth (11) Christmas Day

(6) Independence Day

In addition to the days designated as holidays, the Government observes the following days:

* Any other day designated by Federal Statute.
* Any other day designated by Executive Order.
* Any other day designated by the President's Proclamation

No work shall be performed by Contractor personnel at Government facilities

on Federal holidays or other nonwork days without prior written approval of the CO.

It is understood and agreed between the Government and the Contractor that observance of such days by Government personnel shall not otherwise be a reason for an additional period of performance, or entitlement of compensation except as set forth within the contract. In the event the Contractor's personnel work during the holiday, they may be reimbursed by the Contractor, however, no form of holiday or other premium compensation will be reimbursed either as a direct or indirect cost, other than their normal compensation for the time worked. This provision does not preclude reimbursement for authorized overtime work if applicable to this contract.

When the Federal and governmental entities grant excused absence to its employees, assigned Contractor personnel may also be dismissed. The Contractor agrees to continue to provide sufficient personnel to perform critical tasks already in operation or scheduled, and shall be guided by the instructions issued by the CO or the COR.

Nothing in this clause abrogates the rights and responsibilities of the parties relating to stop work provisions as cited in other sections of this contract.

Contractor personnel that can continue contract performance (either on-site or at a site other than their normal workstation) shall continue to work and the contract price shall not be reduced or increased.

Contractor personnel that are not able to continue contract performance (e.g., support functions) may be asked to cease their work effort.

Contracting Officer Representative (COR): The COR will be identified by separate letter by the CO. The COR monitors all technical aspects of the contract and assists in contract administration.

The COR is authorized to perform the following functions: assure that the Contractor performs the technical requirements of the contract; perform inspections necessary in connection with contract performance; maintain written and oral communications with the Contractor concerning technical aspects of the contract; issue written interpretations of technical requirements, including Government drawings, designs, and specifications; monitor Contractor's performance and notify both the Contracting Officer and Contractor of any deficiencies; coordinate availability of government furnished property; and provide site entry of Contractor personnel.

A letter of designation issued to the COR, a copy of which is sent to the Contractor, states the responsibilities and limitations of the COR, especially about changes in cost or price, estimates or changes in delivery dates. The COR is not authorized to change any of the terms and conditions of the resulting order.

**16.0 PERFORMANCE REQUIREMENTS SUMMARY (PRS)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Performance Objective** | **Performance Standard** | **Performance Threshold** | **Quality Surveillance Method (Government)** |
| Deliver software that is intuitive and usable to continuously improve the efficiency and effectiveness of website communications and reports | 90 percent or better positive survey comments during user acceptance testing (UAT) | Demonstration during Sprint ReviewApproval by Government Product Owner prior to software release | Planned sampling inspection |
|  Release working software frequently and consistently using agile and iterative processes in response to evolving agency business needs and reduce the time from customer demand to fulfillment | 95 percent of working software releases are released to production within no later than completion of four Sprints (Sprint duration 2-4 weeks each) | Agile Product Owner (Federal I.T. Program Manager) approval to release software | Planned sampling inspection |
| Use a modern technology stack and automated testing to enable website services to scale easily and cost-effectively | 100 percent of the website infrastructure elements within direct control of the Contractor use a modern technology stack, automate open-source software testing to the maximum extent practicable | Contractor (SCRUM Master) makes recommendations to the Government during annual technology “refresh” to upgrade specific elements of the technology stackAutomated testing – 70 percent or more of testing is automated. | Random sampling inspection |
| Deliver defect-free software to the maximum extent practicable | 95 percent or better of software delivered defect free | A minim of four key Agile SCRUM metrics covering process, product, and quality selected by the cross-functional team, and reported at the bi-weekly technical meeting | Random sampling inspection |

**TERMS AND CONDITIONS**

**Section 508 Accessibility Standards**

Contractor shall provide evidence of Section 508 compliance for all information technology products proposed.

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

All products, platforms and services delivered as part of this work statement that are ICT, or contain ICT, must conform to the Revised 508 Standards, which are located at 36 C.F.R. § 1194.1 & Apps. A, B, C & D, and available at <https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/final-rule/text-of-the-standards-and-guidelines>.

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

For each proposed product, platform, or service, a fully completed Accessibility Conformance Report (ACR) using the Voluntary Product Accessibility Template (VPAT) (<https://www.itic.org/policy/accessibility/vpat>) must be submitted. Evaluation will be on an Acceptable/Unacceptable basis.

Prior to acceptance of deliverables, the offeror must demonstrate conformance to the HHS Section 508 requirements via HHS Section 508 checklist(s) (<https://www.hhs.gov/web/section-508/accessibility-checklists/index.html>). The government reserves the right to perform testing on required ICT items to validate the offeror’s Section 508 conformance claims. If the government determines that Section 508 conformance does not meet the HHS Section 508 requirements, the government shall, at its option, require the offeror to remediate the item, at no additional cost to the government, to align with the HHS Section 508 conformance requirements prior to acceptance.

References:
\* Section 508 Standards: <https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/final-rule/text-of-the-standards-and-guidelines>
\* HHS Policy on Section 508 Compliance and Accessibility of Information and Communications Technology (ICT): <https://www.hhs.gov/web/governance/digital-strategy/it-policy-archive/department-of-health-and-human-services-hhs-policy-on-section-508-and-accessibility-of-technology.html>
\* HHS Accessibility and Section 508 Compliance Checklists: <https://www.hhs.gov/web/section-508/accessibility-checklists/index.html>

**Security Requirements:**

Contractor shall complete Information Systems Security Awareness (ISSA) and Privacy Awareness (PA)Training and subsequently read and sign a computer access agreement and rules of behavior to be granted access to the HHS network.

* All work performed under a contract awarded as a result of this solicitation must comply with the HHS Office of the Chief Information Officer policy dated 3 March 2021, “[Security and Privacy Language for Information and Information Technology Procurements](https://intranet.hhs.gov/policy/hhs-policy-information-technology-procurements-security-and-privacy-language#8),” version 3.2. This policy document is on the HHS intranet and is available on request.
* Baseline Security Requirements
	+ **Applicability.**The requirements herein apply whether the entire contract or modification (hereafter "contract"), or portion thereof, includes either or both of the following:
		- **Access (Physical or Logical) to Government Information:** A Contractor (and/or any subcontractor) will have or will be given the ability to have, routine physical (entry) or logical (electronic) access to government information.
		- **Operate a Federal System Containing Information:** A Contractor (and/or any subcontractor) will operate a federal system and information technology containing data that supports the HHS mission. In addition to the Federal Acquisition Regulation (FAR) Subpart 2.1 definition of "information technology" (IT), the term as used in this section includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources.

**Safeguarding Information and Information Systems.** All government information and information systems must be protected in accordance with HHS/*[ASPR]* policies and level of risk. At a minimum, the Contractor (and/or any subcontractor) must:

* + - Protect the:
			* **Confidentiality**, which means preserving authorized restrictions on access and disclosure, based on the security terms found in this contract, including means for protecting personal privacy and proprietary information.
			* **Integrity**, which means guarding against improper information modification or destruction, and ensuring information non-repudiation and authenticity; and
			* **Availability**, which means ensuring timely and reliable access to and use of information.
		- Categorize all information owned and/or collected/managed on behalf of HHS/ *[ASPR]* and information systems that store, process, and/or transmit HHS information in accordance with FIPS 199 and National Institute of Standards and Technology ([NIST) Special Publication (SP) 800-60, Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories.](http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol2-Rev1.pdf)Based on information provided by the ISSO, CISO, ASPR SOP, or other representative, the impact level for each Security Objective (Confidentiality, Integrity, and Availability) and the Overall Impact Level, which is the highest watermark of the three factors of the information or information system are the following:
			* **Confidentiality: [** x ] Low [  ] Moderate [  ] High
			* **Integrity:**  [  ] Low [ x ] Moderate [  ] High
			* **Availability:**[  ] Low [  x] Moderate [  ] High
			* **Overall Impact Level:** [  ] Low [ x ] Moderate [  ] High
		- Based on the agreed-upon level of impact, implement the necessary safeguards to protect all information systems and information collected and/or managed on behalf of HHS*/ [ASPR]*regardless of location or purpose.
		- Report any discovered or unanticipated threats or hazards by either the agency or contractor, or if existing safeguards have ceased to function immediately after discovery, **within one (1) hour or less**, to the government representative(s).
		- Adopt and implement all applicable policies, procedures, controls, and standards required by the HHS/*[ASPR]* Information Security Program to ensure the confidentiality, integrity, and availability of government information and government information systems for which the Contractor is responsible under this contract or to which the Contractor may otherwise have access under this contract. Obtain all applicable security and privacy policies by contacting the CO/COR or HHS/ *[ASPR]* security and/or privacy officials.
	+ **Privacy Act.** Comply with the Privacy Act requirements (when applicable), and tailor FAR and HHSAR clauses as needed.
	+ **Privacy Compliance.** Comply with the E-Government Act of 2002, NIST SP 800-53, and applicable HHS/ASPR privacy policies, and complete all the requirements below:
	*.*
		- Per the Office of Management and Budget (OMB) Circular A-130, Personally Identifiable Information (PII), is "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." Examples of PII include, but are not limited to the following: Social Security number, date and place of birth, mother's maiden name, biometric records, etc.
		- To ensure that the public's personal information is protected in a manner commensurate with the privacy risks, HHS uses a privacy analysis process to assess the risks associated with HHS's collection and maintenance of PII and to ensure information is handled in accordance with applicable legal, regulatory, and policy requirements. PTAs analyze how information is handled in IT systems and electronic information collections and determines if the IT system or electronic information collection collects, disseminates, maintains, or disposes of PII. PIAs are used to assess the privacy risks of IT systems and electronic information collections that collect, disseminate, maintain, or dispose of PII about members of the public. PIAs also provide transparency into how HHS collects, disseminates, maintains, or disposes of the public's PII.
		- The Contractor must support the agency with conducting a Privacy Threshold Analysis (PTA) for the information system and/or information handled under this contract to determine whether PII is collected, disseminated, maintained, or disposed as part of the contract. The PTA will determine if a full Privacy Impact Assessment (PIA) needs to be completed.
			* If the results of the PTA show that a full PIA is needed, the Contractor must support the agency with completing a PIA for the system or information within *60 calendar days* after completion of the PTA and in accordance with HHS policy and OMB M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*.
			* The Contractor must support the agency in reviewing the PIA at least every ***three years*** throughout the system development lifecycle (SDLC)/information lifecycle, or when determined by the agency that a review is required based on a major change to the system, or when new types of PII are collected that introduces new or increased privacy risks, whichever comes first.
	+ **Controlled Unclassified Information (CUI). Executive Order 13556 defines**CUI as "information that laws, regulations, or Government-wide policies require to have safeguarding or dissemination controls, excluding classified information." The Contractor (and/or any subcontractor) must comply with *Executive Order 13556, Controlled Unclassified Information, (implemented at 3 CFR,*part 2002*)* when handling CUI. 32 C.F.R. 2002.4(aa) As implemented the term "*handling"*refers to "…any use of CUI, including but not limited to marking, safeguarding, transporting, disseminating, re-using, and disposing of the information." 81 Fed. Reg. 63323.  The requirements below apply only to nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components. All sensitive information that has been identified as CUI by a regulation or statute, handled by this solicitation/contract, must be:
		- Marked appropriately.
		- Disclosed to authorized personnel on a Need-To-Know basis.
		- Protected in accordance with NIST SP 800-53,*Security and Privacy Controls for Information Systems and Organizations*applicable baseline if handled by a contractor system operated on behalf of the agency, or NIST SP 800-171,*Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations* if handled by internal Contractor system; and
		- Returned to HHS control, destroyed when no longer needed, or held until otherwise directed. Information and/or data must be disposed of in accordance with NIST SP 800-88*, Guidelines for Media Sanitization*.
	+ **Protection of Sensitive Information**. For security purposes, information is *or*may be sensitive because it requires security to protect its confidentiality, integrity, and/or availability. The Contractor (and/or any subcontractor) must protect all government information that is or may be sensitive by securing it with a solution that is validated with current FIPS 140 validation certificates from the NIST CMVP.
	+ **Confidentiality and Nondisclosure of Information**. Any information provided to the contractor (and/or any subcontractor) by HHS or collected by the contractor on behalf of HHS must be used only for the purpose of carrying out the provisions of this contract and must not be disclosed or made known in any manner to any persons except as may be necessary in the performance of the contract. The Contractor assumes responsibility for protection of the confidentiality of Government records and must ensure that all work performed by its employees and subcontractors must be under the supervision of the Contractor. Each Contractor employee or any of its subcontractors to whom any HHS records may be made available or disclosed must be notified in writing by the Contractor that information disclosed to such employee or subcontractor can be used only for that purpose and to the extent authorized herein.

	The confidentiality, integrity, and availability of such information must be protected in accordance with HHS and *[ASPR]* policies. Unauthorized disclosure of information will be subject to the HHS/*[ASPR]* sanction policies and/or governed by the following laws and regulations:
		- 18 U.S.C. 641 (Criminal Code: Public Money, Property or Records).
		- 18 U.S.C. 1905 (Criminal Code: Disclosure of Confidential Information); and
		- 44 U.S.C. Chapter 35, Subchapter I (Paperwork Reduction Act).
	+ **Internet Protocol Version 6 (IPv6).** All procurements using Internet Protocol must comply with OMB Memorandum M-05-22, *Transition Planning for Internet Protocol Version 6 (IPv6)*.
	+ **Information and Communications Technology (ICT).** ICT products and services from prohibited entities/sources must not be used/acquired in compliance with Public Law 115-232, Section 889 Parts A and B, FAR 4.21, FAR 52.204.23, FAR 52.204.24, and FAR 52.204.25. The contractor (and/or any subcontractor) must notify the government if they identify prohibited ICT products and/or services are used during the contract performance.
	+ **Government Websites.** All new and existing public-facing government websites must be securely configured with Hypertext Transfer Protocol Secure (HTTPS) using the most recent version of Transport Layer Security (TLS). In addition, HTTPS must enable HTTP Strict Transport Security (HSTS) to instruct compliant browsers to always assume HTTPS to reduce the number of insecure redirects and protect against attacks that attempt to downgrade connections to plain HTTP. For internal-facing websites, HTTPS is not required, but it is highly recommended. Consult the *HHS Policy for Internet and Email Security* for additional information.
	+ **Contract Documentation**. The Contractor must use provided templates, policies, forms, and other agency documents to comply with contract deliverables as appropriate.
	+ **Standard for Encryption.**The Contractor (and/or any subcontractor) must:
		- Comply with the *HHS Standard for Encryption of Computing Devices and Information*to prevent unauthorized access to government information.
		- Encrypt all sensitive federal data and information (i.e., PII, protected health information [PHI], proprietary information, etc.) in transit (i.e., email, network connections, etc.) and at rest (i.e., servers, storage devices, mobile devices, backup media, etc.) with encryption solution that is validated with current FIPS 140 validation certificates from the NIST CMVP.
		- Secure all devices (i.e.: desktops, laptops, mobile devices, etc.) that store and process government information and ensure devices meet HHS and ASPR-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).
		- Verify that the encryption solutions in use have been validated under the Cryptographic Module Validation Program to confirm compliance with current FIPS 140 validation certificates from the NIST CMVP. The Contractor must provide a written copy of the validation documentation to the COR *[ASPR-provided delivery date]*.
		- Use the Key Management system on the HHS personal identification verification (PIV) card or establish and use a key recovery mechanism to ensure the ability for authorized personnel to encrypt/decrypt information and recover encryption keys <http://csrc.nist.gov/publications/>. Encryption keys must be provided to the COR upon request and at the conclusion of the contract.
	+ **Contractor Non-Disclosure Agreement (NDA)**. Each Contractor (and/or any subcontractor) employee having access to non-public government information under this contract must complete the ASPR non-disclosure agreement, as applicable. Contractors (and/or subcontractors) must submit a copy of each signed and witnessed NDA to the Contracting Officer (CO) and/or CO Representative (COR) prior to performing any work under this acquisition.
* Training Requirements
	+ **Mandatory Training for All Contractor Staff.** All Contractor (and/or any subcontractor) employees assigned to work on this contract must complete the applicable HHS/ASPR Contractor Information Security Awareness, Privacy, and Records Management training (provided upon contract award) before performing any work under this contract. Thereafter, the employees must complete Information Security Awareness, Privacy, and Records Management training at least ***annually***, during the life of this contract. All provided training must be compliant with HHS training policies.
	+ **Role-based Training.** All Contractor (and/or any subcontractor) employees with significant security responsibilities (as determined by the program manager) must complete role-based training ***annually*** commensurate with their role and responsibilities in accordance with HHS policy and the *HHS Role-Based Training (RBT) of Personnel with Significant Security Responsibilities Memorandum*.
	+ **Training Records.** The Contractor (and/or any subcontractor) must maintain training records for all its employees working under this contract in accordance with HHS policy. A copy of the training records must be provided to the CO and/or COR within ***30 days*** after contract award and ***annually*** thereafter or upon request.
* Rules of Behavior
	+ The Contractor (and/or any subcontractor) must ensure that all employees performing on the contract comply with the *HHS Information Technology General Rules of Behavior*, *HHS Rules of Behavior for Privileged Users*, and [*insert any ASPR-specific rules, as applicable*].
	+ 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 ASPR Information Security Awareness Training. If the training is provided by the contractor, the signed ROB must be provided as a separate deliverable to the CO and/or COR per defined timelines above.
* Incident Response
	+ The Contractor (and/or any subcontractor) must respond to all alerts/Indicators of Compromise (IOCs) provided by HHS Computer Security Incident Response Center (CSIRC)/*[ASPR]* IRT teams **within 24 hours,** whether the response is positive or negative. In accordance with FISMA and OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information (PII)*, an incident is "an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies" and a privacy breach is "the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose." For additional information on the HHS breach response process, please see the *HHS Policy and Plan for Preparing for and Responding to a Breach of Personally Identifiable Information (PII)*."
	+ In the event of a suspected or confirmed incident or breach, the Contractor (and/or any subcontractor) must:
		- Protect all sensitive information, including any PII created, stored, or transmitted in the performance of this contract, with encryption solution that is validated with current FIPS 140 validation certificates from the NIST CMVP.
		- NOT notify affected individuals unless so instructed by the Contracting Officer or designated representative. If so, instructed by the Contracting Officer or representative, the Contractor must send *ASPR* approved notifications to affected individuals *within 5 business days via secure email or registered mail*.
		- Report all suspected and confirmed information security and privacy incidents and breaches to the ASPR Incident Response Team (IRT) , COR, CO, ASPR SOP (or his or her designee), and other stakeholders, including breaches involving PII, in any medium or form, including paper, oral, or electronic, as soon as possible and without unreasonable delay, no later than **one (1) hour**, and consistent with the applicable ASPR and HHS policy and procedures, NIST standards and guidelines, as well as US-CERT notification guidelines. The types of information required in an incident report must include at a minimum: company and point of contact information, contact information, impact classifications/threat vector, and the type of information compromised. In addition, the Contractor must:
			* Cooperate and exchange any information, as determined by the Agency, necessary to effectively manage or mitigate a suspected or confirmed breach.
			* Not include any sensitive information in the subject or body of any reporting e-mail; and
			* Encrypt sensitive information in attachments to email, media, etc.
		- Comply with OMB M-17-12, *Preparing for and responding to a Breach of Personally Identifiable Information,* and HHS/ASPR and *[ASPR]* privacy breach response policies when handling PII breaches.
		- Provide full access and cooperate on all activities as determined by the Government to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents. This may involve disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls. This may also involve physical access to contractor facilities during a breach/incident investigation. ASPR timeline for contractors to provide full access is within 8 business hours.
* Position Sensitivity Designations

All Contractor (and/or any subcontractor) employees must obtain a background investigation commensurate with their position sensitivity designation that complies with Parts 1400 and 731 of Title 5, Code of Federal Regulations (CFR). The following position sensitivity designation levels apply to this solicitation/contract: **Tier 2, Moderate Risk Public Trust.**
* Homeland Security Presidential Directive (HSPD)-12

The Contractor (and/or any subcontractor) and its employees must comply with Homeland Security Presidential Directive (HSPD)-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*; OMB M-05-24; OMB M-19-17; FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*; HHS HSPD-12 policy; and*Executive Order 13467, Part 1 §1.2.*
* Roster

The Contractor (and/or any subcontractor) must submit a roster by name, position, e-mail address, phone number and responsibility, of all staff working under this acquisition where the Contractor will develop, can access, or host and/or maintain a government information system(s). The roster must be submitted to the COR and/or CO within *10 business days* of the effective date of this contract. Any revisions to the roster because of staffing changes must be submitted within *3 business days* of the change. The COR will notify the Contractor of the appropriate level of investigation required for each staff member. *[If the ASPR has an electronic template, include that information here along with a link, if applicable.]*

If the employee is filling a new position, the Contractor must provide a position description and the Government will determine the appropriate suitability level.
* Contract Initiation and Expiration
	+ **General Security Requirements.** The Contractor (and/or any subcontractor) must comply with information security and privacy requirements, Enterprise Performance Life Cycle (EPLC) processes, HHS Enterprise Architecture requirements to ensure information is appropriately protected from initiation to expiration of the contract. All information systems development or enhancement tasks supported by the contractor must follow the HHS EPLC framework and methodology or and in accordance with the HHS Contract Closeout Guide (2012).
	+ **System Documentation.** Contractors (and/or any subcontractors) must follow and adhere to HHS System Development Life Cycle requirements, at a minimum, for system development and provide system documentation at designated intervals (specifically, at the expiration of the contract) within the EPLC that require artifact review and approval.
	+ **Sanitization of Government Files and Information.**As part of contract closeout and at expiration of the contract, the Contractor (and/or any subcontractor) must provide all required documentation to the CO and/or COR to certify that, at the government's direction, all electronic and paper records are appropriately disposed of and all devices and media are sanitized in accordance with NIST SP 800-88, *Guidelines for Media Sanitization*.
	+ **Notification.** The Contractor (and/or any subcontractor) must notify the CO and/or COR and system ISSO within *30 calendar days* before key personnel and *15 calendar days* all other employee stops working under this contract.
	+ **Contractor Responsibilities upon Physical Completion of the Contract**. The contractor (and/or any subcontractors) must return all government information and IT resources (i.e., government information in non-government-owned systems, media, and backup systems) acquired during the term of this contract to the CO and/or COR. Additionally, the Contractor must provide a certification that all government information has been properly sanitized and purged from Contractor-owned systems, including backup systems and media used during contract performance, in accordance with HHS and/or *[ASPR]* policies.
	+ The Contractor (and/or any subcontractor) must perform and document the actions identified in the ASPRContractor Employee Separation Checklist when an employee terminates work under this contract within *3 business days* of the employee's exit from the contract. All documentation must be available to the CO and/or COR upon request.
* Records Management and Retention
	+ The Contractor (and/or any subcontractor) must maintain all information in accordance with Executive Order 13556 -- Controlled Unclassified Information, National Archives and Records Administration (NARA) records retention policies and schedules and *HHS Policy for Records Management* and*[ASPR]* policies and must not dispose of any records unless authorized by HHS*/[ASPR]*.
	+ If a contractor (and/or any subcontractor) accidentally disposes of or destroys a record without proper authorization, he/she must document and report the incident in accordance with HHS*/ [ASPR]* policies.
* High Value Asset (HVA)

If a system is identified as HVA, [[23]](https://intranet.hhs.gov/policy/hhs-policy-information-technology-procurements-security-and-privacy-language#ftn23) the contractor must comply with the HHS Policy for the High Value Asset (HVA) Program and the DHS HVA Control Overlay [[24]](https://intranet.hhs.gov/policy/hhs-policy-information-technology-procurements-security-and-privacy-language#ftn24) in addition to the above requirements.

Privacy Act

It has been determined that this contract is subject to the Privacy Act of 1974, because this contract provides for the design, development, or operation of a system of records about individuals from which records are retrieved by name or other identifying.

The System of Records Notice that is applicable to the ASPR Web Environment will be developed during the period of the task order.

The system of records design, development, or operation work the Contractor is to perform is to advise the ASPR COR. ASPR COR will subsequently consult with the ASPR Privacy Office.

The disposition to be made of the Privacy Act records upon completion of contract performance is return all official records to ASPR.

Privacy Act Notification (Apr 1984)

The Contractor will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of1974, Public Law93-579, December 31,1974 ([5 U.S.C.552a](http://uscode.house.gov/browse.xhtml;jsessionid=114A3287C7B3359E597506A31FC855B3)) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties.

Privacy Act (Apr 1984)

      (a) The Contractor agrees to-

           (1) Comply with the Privacy Act of1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies-

                (I) The systems of records.

                (ii) The design, development, or operation work that the contractor is to perform.

           (2) Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a system of records on individuals that is subject to the Act; and

           (3) Include this clause, including this paragraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a system of records.

      (b) In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a system of records on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a system of records on individuals to accomplish an agency function, the Contractor is an employee of the agency.

(1) "Operation of a system of records," as used in this clause, means performance of any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of records.

           (2) "Record," as used in this clause, means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and that contains the person’s name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint or voiceprint or a photograph.

           (3) "System of records on individuals," as used in this clause, means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying assigned to the individual.

1. Security Requirements for GOCO and COCO Resources
	1. **Federal Policies.**The Contractor (and/or any subcontractor) must comply with applicable federal laws and HHS policies that include, but are not limited to, the *HHS Information Security and Privacy Policy (IS2P)da*; *Federal Information Security Modernization Act (FISMA) of 2014, (44 U.S.C. 101)*; National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, latest revision, *Security and Privacy Controls for Information Systems and*Organizations; Office of Management and Budget (OMB) Circular A-130*, Managing Information as a Strategic Resource*; and other applicable federal laws, regulations, NIST guidance, and Departmental policies.
	2. **Assessment and Authorization (A&A)**. A valid authority to operate (ATO) certifies that the Contractor's information system meets the contract's requirements to protect the agency data. If the system under this contract does not have a valid ATO, the Contractor (and/or any subcontractor) must work with the agency and supply the deliverables required to complete the ATO within the specified timeline of 180 calendar days. The Contractor must conduct the A&A requirements in accordance with *HHS IS2PD-12,* NIST SP 800-37, *and Guide for Applying the Risk Management Framework to Information Systems: A Security Life Cycle Approach*(latest revision), NIST SP 800-53B, *Control Baselines for Information Systems and Organizations*, and the NIST SP 800-53A (latest revision).

	***Note to the Requiring Activity Representative:****For an existing ATO, the ASPR must make a determination if the system needs to be re-authorized to ensure all necessary* safeguards *are in place to protect the system and information for the performance of the contract and state as such.*

	*ASPR* acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the system security and privacy controls are implemented and operating effectively.
		1. **A&A Package Deliverables** - The Contractor (and/or any subcontractor) must provide an A&A package within *90 calendar days* to the CO and/or COR. The following A&A deliverables are required to complete the A&A package:
			* **System Security Plan (SSP)** - due *90 calendar days to the CO and/or COR in Microsoft Office format*. The SSP must comply with the NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, the Federal Information Processing Standard (FIPS) 200, *Recommended Security Controls for Information Systems*, and NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* applicable baseline requirements, and other applicable NIST guidance as well as HHS and *[ASPR]* policies and other guidance. The SSP must be consistent with and detail the approach to IT security contained in the Contractor's bid or proposal that resulted in the award of this contract. The SSP must provide an overview of the system environment and security requirements to protect the information system as well as describe all applicable security controls in place or planned for meeting those requirements. It should provide a structured process for planning adequate, cost-effective security protection for a system. The Contractor must review and update the SSP at least ***annually*** thereafter and if requested, provide a copy of the updated SSP.
			* **Security Assessment Plan/Report (SAP/SAR)** - due *90 calendar days after contract award in Microsoft Office format.]*The security assessment must be conducted by *a qualified cyber security* assessor and be consistent with NIST SP 800-53A, NIST SP 800-30, and HHS and ASPR policies. The assessor will document the assessment results in the SAR.

			Thereafter, the Contractor, in coordination with *ASPR System Owner**and**ASPR CISO*must *assist* in the assessment of the security controls and update the SAR at least ***annually***. A copy of the updated SAR should be provided if requested.
			* **Independent Assessment -** due *within 90 days of contract award if the information system is not already in ATO approved status The ASPR Web Environment ATO is current as of July 2021 and is not due for renewal for 2 years.* The Contractor (and/or subcontractor) must have an independent third-party validate the security and privacy controls in place for the system(s) commensurate with the risk levels per NIST SP 800-53B. The independent third party must review and analyze the Security Authorization package, and report on technical, operational, and management level deficiencies as outlined in NIST SP 800-53. The Contractor must address all *"high"* deficiencies before submitting the package to the Government for acceptance and document all remaining deficiencies in a system Plan of Actions and Milestones (POA&M).
			* **POA&M** - due *90 days after contract award in Microsoft Office format, to be entered into the ASPR ARCHER risk management system*. All critical-risk weaknesses must be mitigated within *[15 calendar days]*, high-risk weaknesses must be mitigated within *[30 calendar days]*, medium weaknesses must be mitigated within [90 *calendar days*], and low weaknesses must be mitigated within *360 calendar days]]*, from the date the weaknesses are formally identified and documented. *[ASPR]* will determine the risk rating of vulnerabilities. Identified risks stemming from deficiencies related to the security control baseline implementation, assessment, continuous monitoring, vulnerability scanning, flaws, and security defect in a system (that require to create a patch for remediation), and other security reviews and sources, as documented in the SAR, must be documented, and tracked by the Contractor for mitigation in the POA&M document consistent with the HHS Standard for Plan of Action and Milestones and ASPR policies. Depending on the severity of the risks, *[ASPR]* may require designated POA&M weaknesses to be remediated before an ATO is issued. Thereafter, continue to remediate weaknesses throughout the contract. The POA&M document must be updated at least **quarterly***.*
			* **Contingency Plan and Contingency Plan Test** - The Contingency Plan must be developed in accordance with NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems*, and be consistent with HHS and ASPR policies. Upon acceptance by the System Owner, the Contractor, in coordination with the System Owner, must test the Contingency Plan and prepare a Contingency Plan Test Report that includes the test results, lessons learned and any action items that need to be addressed. Contractor must update and test the Contingency Plan at least ***annually***.
			* **E-Authentication Questionnaire** - The contractor (and/or any subcontractor) must collaborate with government personnel to ensure that the E-Authentication requirements are implemented in accordance with OMB 04-04 and NIST SP 800-63 B.

			Based on the level of assurance determined by the E-Auth, the Contractor (and/or subcontractor) must ensure appropriate authentication to the system, including remote authentication, is in-place in accordance with the assurance level determined by the E-Auth (when required) in accordance with HHS *Guidance for Selection of e-Authentication Assurance Levels* and any other applicable HHS policies.
		2. **Information Security Continuous Monitoring.**Upon the government issuance of an Authority to Operate (ATO), the Contractor (and/or subcontractor)-owned/operated systems that input, store, process, output, and/or transmit government information, must meet, or exceed the information security continuous monitoring (ISCM) requirements in accordance with FISMA and NIST SP 800-137*, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, HHS ISCM Strategy, and HHS IS2P.
		3. **Annual Assessment/Penetration (Pen) Test -** Assess the system security and privacy controls (or ensure an assessment of the controls is conducted) at least annually to determine the implemented security and privacy controls are operating as intended and producing the desired results (this involves penetration testing conducted by the agency or independent third-party.) In addition, review all relevant A&A documentation (SSP, POA&M, Contingency Plan, etc.) and provide updates by specified due date.
		4. **Asset Management -** Using any available Security Content Automation Protocol (SCAP)-compliant automated tools for active/passive scans, provide an inventory of all information technology (IT) assets for hardware and software, (computers, servers, routers, databases, operating systems, etc.) that are processing HHS-owned information/data. It is anticipated that this inventory information will be required to be produced at least*annually.* IT asset inventory information must include IP address, machine name, operating system level, security patch level, and SCAP-compliant format information. The contractor must maintain a capability to provide an inventory of 100% of its IT assets using SCAP-compliant automated tools in accordance with the *HHS Policy for Information Technology Asset Management (ITAM)* and any other applicable HHS policy.
		5. **Configuration Management -** Use available SCAP-compliant automated tools as per NIST IR 7511 and *HHS Minimum Security Configurations Standards Guidance* to scan all IT assets, including but not limited to: computers, servers, routers, databases, operating systems, application, etc., that store and process government information. Provide scan reports to HHS*/ [ASPR]* upon request. The contractor must maintain a capability to provide security configuration compliance information for 100% of its IT assets using SCAP-compliant automated tools.
		6. **Vulnerability Management -** Contractors must actively manage system vulnerabilities using automated tools and technologies where practicable and in accordance with *HHS Policy for Vulnerability Management*. Automated tools must be compliant with NIST-specified SCAP standards for vulnerability identification and management. The contractor must maintain a capability to provide security vulnerability scanning information for 100% of IT assets using SCAP-compliant automated tools and report to the agency at least *[insert specific timeframe]*.
		7. **Patching and Vulnerability Remediation -** Install vendor released security patches and remediate critical and high vulnerabilities in systems processing government information in an expedited manner, within vendor and agency specified timeframes. ASPR CISO will advise on specified timeframes.
		8. **Secure Coding -** Follow the *HHS Policy for Software Development Secure Coding Practices* and secure coding best practice requirements, as directed by United States Computer Emergency Readiness Team (US-CERT) specified standards and the Open Web Application Security Project (OWASP), that will limit system software vulnerability exploits.
		9. **Boundary Protection -** The contractor must ensure that government information, other than unrestricted information, being transmitted from federal government entities to external entities is routed through a Trusted Internet Connection (TIC).
	3. **Government Access for Security Assessment**. In addition to the Inspection Clause in the contract, the Contractor (and/or any subcontractor) must afford the Government access to the Contractor's facilities, installations, operations, documentation, information systems, and personnel used in performance of this contract to the extent required to carry out a program of security assessment (to include vulnerability testing), investigation, and audit to safeguard against threats and hazards to the confidentiality, integrity, and availability of federal data or to the protection of information systems operated on behalf of HHS, including but are not limited to:
		1. At any tier handling or accessing information, consent to and allow the Government, or an independent third party working at the Government's direction, without notice at any time during a weekday during regular business hours contractor local time, to access contractor and subcontractor installations, facilities, infrastructure, data centers, equipment (including but not limited to all servers, computing devices, and portable media), operations, documentation (whether in electronic, paper, or other forms), databases, and personnel which are used in performance of the contract.

		The Government includes but is not limited to the U.S. Department of Justice, U.S. Government Accountability Office, and the HHS Office of the Inspector General (OIG). The purpose of the access is to facilitate performance inspections and reviews, security and compliance audits, and law enforcement investigations. For security audits, the audit may include but not be limited to such items as buffer overflows, open ports, unnecessary services, lack of user input filtering, cross site scripting vulnerabilities, SQL injection vulnerabilities, and any other known vulnerabilities.
		2. At any tier handling or accessing protected information, fully cooperate with all audits, inspections, investigations, forensic analysis, or other reviews or requirements needed to carry out requirements presented in applicable law or policy. Beyond providing access, full cooperation also includes, but is not limited to, disclosure to investigators of information sufficient to identify the nature and extent of any criminal or fraudulent activity and the individuals responsible for that activity. It includes timely and complete production of requested data, metadata, information, and records relevant to any inspection, audit, investigation, or review, and making employees of the contractor available for interview by inspectors, auditors, and investigators upon request. Full cooperation also includes allowing the Government to make reproductions or copies of information and equipment, including, if necessary, collecting a machine or system image capture.
			* Segregate Government protected information and metadata on the handling of Government protected information from other information. Commingling of information is prohibited. Inspectors, auditors, and investigators will not be precluded from having access to the sought information if sought information is commingled with other information.
			* Cooperate with inspections, audits, investigations, and reviews.
	4. **End of Life Compliance.** The Contractor (and/or any subcontractor) must use Commercial off the Shelf (COTS) software or other software that is supported by the manufacturer. In addition, the COTS/other software need to be within one major version of the current version; deviation from this requirement will only be allowed via the HHS waiver process (approved by HHS CISO if it impacts enterprise-wide systems and services, or by the ASPR CISO if it impacts only the ASPR). The contractor must retire and/or upgrade all software/systems that have reached end-of-life in accordance with *HHS End of Life Operating Systems, Software and Application Policy*.
	5. **Desktops, Laptops, and Other Computing Devices Required for Use by the Contractor**. The Contractor (and/or any subcontractor) must ensure that all IT equipment (e.g., laptops, desktops, servers, routers, mobile devices, peripheral devices, etc.) used to process information on behalf of HHS are deployed and operated in accordance with approved security configurations and meet the following minimum requirements:
		1. Encrypt equipment and sensitive information stored and/or processed by such equipment in accordance with HHS encryption standard and current FIPS 140 validation certificates from the NIST CMVP.
		2. Configure laptops and desktops in accordance with the latest applicable United States Government Configuration Baseline (USGCB), *[ASPR insert specific security configuration baseline if any]*, and HHS Minimum Security Configuration Standards.
		3. Maintain the latest operating system patch release and anti-virus software definitions *monthly*.
		4. Validate the configuration settings after hardware and software installation, operation, maintenance, update, and patching and ensure changes in hardware and software do not alter the approved configuration settings; and
		5. Automate configuration settings and configuration management in accordance with HHS security policies, including but not limited to:
			* Configuring its systems to allow for periodic HHS vulnerability and security configuration assessment scanning; and
			* Using Security Content Automation Protocol (SCAP)-validated tools with capabilities to scan its systems at least monthly and report the results of these scans to the CO and/or COR, Project Officer, and any other applicable designated POC.
	6. **Rights to Data.** All contracts that require data to be produced, furnished, acquired, or used in meeting contract performance requirements, must contain terms that delineate the respective rights and obligations of the Government and the contractor regarding the use, reproduction, and disclosure of that data. Data rights clauses do not specify the type, quantity or quality of data that is to be delivered, but only the respective rights of the Government and the contractor regarding the use, disclosure, or reproduction of the data. Accordingly, the contract must specify the data to be delivered.
	7. **Information and Communications Technology (ICT) Cybersecurity Supply Chain Risk Management (C-SCRM) requirements**. The Contractor (and/or any subcontractor) must secure their ICT supply chain in compliance with *HHS Policy for Cyber Supply Chain Risk Management* and Public Law 115-232 § 889. At a minimum, they must implement the following:
		1. Develop rules for suppliers' development methods, techniques, or practices.
		2. Use of secondary market components.
		3. Prohibit counterfeit products.
		4. Dispose and/or retain elements such as components, data, or intellectual property securely.
		5. Ensure adequate supply of components.
		6. Require external providers handling federal information or operating systems on behalf of the federal government to meet the same security and privacy requirements as federal agencies.
		7. Require external providers to express security and privacy requirements (including the controls for systems processing, storing, or transmitting federal information) in contracts or other formal agreements.
		8. Establish Service Level Agreements (SLAs), patching vehicles and disclosure requirements in the case of a security incident or new vulnerability being discovered; and
		9. Ensure that the supplier applies same contractual requirements to any sub-contractors/suppliers that they involve in the provision of the product or service to the customer; and
		10. Prohibit the use of covered telecommunications and video surveillance equipment or services.
2. HHS Fed RAMP Privacy and Security Requirements

The Contractor (and/or any subcontractor) must be responsible for the following privacy and security requirements:
	1. **Fed RAMP Compliant ATO**. Comply with Fed RAMP Assessment and Authorization (A&A) requirements and ensure the information system/service under this contract has a valid Fed RAMP compliant (approved) authority to operate (ATO) in accordance with Federal Information Processing Standard (FIPS) Publication 199 defined security categorization. If a Fed RAMP compliant ATO has not been granted, the Contractor must submit a plan to obtain a Fed RAMP compliant ATO by *[insert specific timeframe, process, and format for contractor to submit ATO package and/or deliverables]*.
		1. Implement applicable Fed RAMP baseline controls commensurate with the agency-defined security categorization and the applicable Fed RAMP security control baseline ([www.FedRAMP.gov](http://www.fedramp.gov/)). The *HHS Information Security and Privacy Policy (IS2P)* and *HHS Cloud Computing and Federal Risk and Authorization Management Program (Fed RAMP) Guidance* further define the baseline policies as well as roles and responsibilities. The Contractor must also implement a set of additional controls identified by the agency when applicable.
		2. A security control assessment must be conducted by a Fed RAMP third-party assessment organization (3PAO) for the initial ATO and ***annually*** thereafter or whenever there is a significant change to the system's security posture in accordance with the Fed RAMP Continuous Monitoring Plan.
	2. **Data Jurisdiction.** The contractor must store all information within the security authorization boundary, data at rest or data backup, within the Continental United States (CONUS) if so required *[ASPR CISO defines locations and boundaries]*.
	3. **Service Level Agreements.** The Contractor must understand the terms of the service agreements that define the legal relationships between cloud customers and cloud providers and work with *[ASPR]* to develop and maintain an SLA.
	4. **Interconnection Agreements/Memorandum of Agreements.**The Contractor must establish and maintain Interconnection Agreements and or Memorandum of Agreements/Understanding in accordance with HHS/ *[ASPR]*policies. ASPR Web Environment provides identity and authentication services to the National Disaster Medical System (NDMS) intermittent medical professionals via a Memorandum of Understanding (MOU) <https://ams.hhs.gov> .
3. Protection of Information in a Cloud Environment
	1. If contractor (and/or any subcontractor) personnel must remove any information from the primary work area, they must protect it to the same extent they would the proprietary data and/or company trade secrets and in accordance with HHS policies <https://www.hhs.gov/web/governance/digital-strategy/it-policy-archive/index.html>.
	2. HHS will retain unrestricted rights to federal data handled under this contract. Specifically, HHS retains ownership of any user created/loaded data and applications collected, maintained, used, or operated on behalf of HHS and hosted on contractor's infrastructure, as well as maintains the right to request full copies of these at any time. If requested, data must be available to HHS within ***one (1) business day*** from request date or within the timeframe specified otherwise. In addition, the data must be provided at no additional cost to HHS.
	3. The Contractor (and/or any subcontractor) must ensure that the facilities that house the network infrastructure are physically and logically secure in accordance with Fed RAMP requirements and HHS policies.
	4. The contractor must support a system of records in accordance with NARA-approved records schedule(s) and protection requirements for federal agencies to manage their electronic records in accordance with 36 CFR § 1236.20 & 1236.22 (ref. a), including but not limited to the following:
		1. Maintenance of links between records and metadata, and
		2. Categorization of records to manage retention and disposal, either through transfer of permanent records to NARA or deletion of temporary records in accordance with NARA-approved retention schedules.
	5. The disposition of all HHS data must be at the written direction of HHS/ *[ASPR]*. This may include documents returned to HHS control; destroyed; or held as specified until otherwise directed. Items returned to the Government must be hand carried or sent by certified mail to the COR.
		1. If the system involves the design, development, or operation of a system of records on individuals, the Contractor must comply with the Privacy Act requirements*[ASPR CISO include Privacy Act language from Appendix B: Standards]*.
4. Assessment and Authorization (A&A) Process
	1. The Contractor (and/or any subcontractor) must comply with HHS and Fed RAMP requirements as mandated by federal laws, regulations, and HHS policies, including making available any documentation, physical access, and logical access needed to support the A&A requirement. The level of effort for the A&A is based on the system's FIPS 199 security categorization and HHS*/ [ASPR]* security policies. Certification requirements are defined by the HHS Fed RAMP Office.
		1. In addition to the Fed RAMP compliant ATO, the contractor must complete and maintain an agency A&A package to obtain agency ATO prior to system deployment/service implementation. The agency ATO must be approved by the *[ASPR]* authorizing official (AO) prior to implementation of system and/or service being acquired.
		2. CSP systems categorized as Federal Information Processing Standards (FIPS) 199 high must leverage a Fed RAMP accredited third-party assessment organization (3PAO); moderate impact CSP systems must make a best effort to use a Fed RAMP accredited 3PAO but should not use self-assessment. CSP systems categorized as FIPS 199 low impact may leverage a non-accredited, independent assessor.
		3. For all acquired cloud services, the A&A package must contain the following required documentation. Following the initial ATO, the Contractor must review and maintain the ATO in accordance with HHS*/ [ASPR]* policies. The ASPR Web Environment ATO is current as of 15 July 2021, ATO renewal is not due for 3 years.
	2. HHS reserves the right to perform penetration testing (pen testing) on all systems operated on behalf of agency. If HHS exercises this right, the Contractor (and/or any subcontractor) must allow HHS employees (and/or designated third parties) to conduct Security Assessment activities to include control reviews in accordance with HHS requirements. Review activities include, but are not limited to, scanning operating systems, web applications, wireless scanning; network device scanning to include routers, switches, and firewall, and IDS/IPS; databases and other applicable systems, including general support structure, that support the processing, transportation, storage, or security of Government information for vulnerabilities.
	3. The Contractor must identify any gaps between required Fed RAMP Security Control Baseline/Continuous Monitoring controls and the contractor's implementation status as documented in the Security Assessment Report and related Continuous Monitoring artifacts. In addition, the contractor must document and track all gaps for mitigation in a Plan of Action and Milestones (POA&M) document. Depending on the severity of the risks, HHS may require remediation at the contractor's expense before HHS issues an ATO.
	4. The Contractor (and/or any subcontractor) must mitigate security risks for which they are responsible, including those identified during A&A and continuous monitoring activities. All vulnerabilities and findings must be remediated, in accordance with timelines specified in the HHS POA&M Standard, from discovery: (1) critical vulnerabilities no later than ***fifteen (15) days*** and (2) high within **thirty (30) days** (3) medium within **ninety (90) days** and (4) low vulnerabilities no later ***than three hundred and sixty (360) days****.*In the event a vulnerability or other risk finding cannot be mitigated within the prescribed timelines above, they must be added to the designated POA&M and mitigated within the newly designated timelines. HHS will determine the risk rating of vulnerabilities using Fed RAMP baselines.
	5. **Revocation of a Cloud Service**. HHS*/ [ASPR]* have the right to act in response to the CSP's lack of compliance and/or increased level of risk. In the event the CSP fails to meet HHS and Fed RAMP security and privacy requirements and/or there is an incident involving sensitive information, HHS and/or *[ASPR]* may suspend or revoke an existing agency ATO (either in part or in whole) and/or cease operations. If an ATO is suspended or revoked in accordance with this provision, the CO and/or COR may direct the CSP to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor information system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.
5. Reporting and Continuous Monitoring
	1. Following the initial ATOs, the Contractor (and/or any subcontractor) must perform the minimum ongoing continuous monitoring activities specified below, submit required deliverables by the specified due dates, and meet with the system/service owner and other relevant stakeholders to discuss the ongoing continuous monitoring activities, findings, and other relevant matters. The CSP will work with the agency to schedule ongoing continuous monitoring activities.
	2. At a minimum, the Contractor must provide the following artifacts/deliverables monthly:
		1. Operating system, database, Web application, and network vulnerability scan results.
		2. Updated POA&Ms.
		3. Any updated authorization package documentation as required by the annual attestation/assessment/review or as requested by the *[ASPR]* System Owner or AO, and.
		4. Any configuration changes to the system and/or system components or CSP's cloud environment, that may impact HHS/ *[ASPR]*'s security posture. Changes to the configuration of the system, its components, or environment that may impact the security posture of the system under this contract must be approved by the agency.
6. Configuration Baseline
	1. The contractor must certify that applications are fully functional and operate correctly as intended on systems using *HHS Minimum Security Configurations Standards Guidance*. The standard installation, operation, maintenance, updates, and/or patching of software must not alter the configuration settings from the approved HHS*/ [ASPR] [enter ASPR CISO Specific configuration requirements]* configuration baseline.
	2. The contractor must use Security Content Automation Protocol (SCAP) validated tools with configuration baseline scanner capability to certify their products operate correctly with HHS and NIST defined configurations and do not alter these settings.
7. Incident Reporting

	1. The Contractor (and/or any subcontractor) must provide an Incident and Breach Response Plan (IRP) in accordance with HHS *[ASPR]*, OMB, and US-CERT requirements and obtain approval from the ASPR. In addition, the Contractor must follow the incident response and US-CERT reporting guidance contained in the Fed RAMP Incident Communications.
	2. The Contractor (and/or any subcontractor) must implement a program of inspection to safeguard against threats and hazards to the security, confidentiality, integrity, and availability of federal data, afford HHS access to its facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of notification. The program of inspection must include, but is not limited to:
		1. Conduct authenticated and unauthenticated operating system/network/database/Web application vulnerability scans. Automated scans can be performed by HHS*/ [ASPR]* personnel, or agents acting on behalf of HHS/ *[ASPR],*using agency-operated equipment and/or specified tools. The Contractor may choose to run its own automated scans or audits, provided the scanning tools and configuration settings are compliant with NIST Security Content Automation Protocol (SCAP) standards and have been approved by the agency. The agency may request the Contractor's scanning results and, at the agency discretion, accept those in lieu of agency performed vulnerability scans.
		2. In the event an incident involving sensitive information occurs, cooperate on all required activities determined by the agency to ensure an effective incident, or breach response and provide all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents. In addition, the Contractor must follow the agency reporting procedures and document the steps it takes to contain and eradicate the incident, recover from the incident, and provide a post-incident report that includes at a minimum the following:
			* Company and point of contact name.
			* Contract information.
			* Impact classifications/threat vector.
			* Type of information compromised.
			* A summary of lessons learned; and
			* Explanation of the mitigation steps of exploited vulnerabilities to prevent similar incidents in the future.
8. Media Transport
	1. The Contractor and its employees must be accountable and document all activities associated with the transport of government information, devices, and media transported outside controlled areas and/or facilities. These include information stored on digital and non-digital media (e.g., CD-ROM, tapes, etc.), mobile/portable devices (e.g., USB flash drives, external hard drives, and SD cards).
	2. All information, devices and media must be encrypted with HHS-approved encryption mechanisms to protect the confidentiality, integrity, and availability of all government information transported outside of controlled facilities.
9. Boundary Protection: Trusted Internet Connections (TIC)
	1. The contractor must ensure that government information, other than unrestricted information, being transmitted from federal government entities to external entities using cloud services is inspected by Trusted Internet Connection (TIC) processes that follow the requirements of the Office of Management and Budget (OMB) Memorandum (M) 19-26: Update to the TIC Initiative, TIC 3.0.
	2. The contractor must route all external connections through a TIC.
	3. **Non-Repudiation**. The contractor must provide a system that implements encryption with current FIPS 140 validation certificates from the NIST CMVP that provides for origin authentication, data integrity, and signer non-repudiation.

 Hardware Procurements

1. **Card Readers**. The Contractor (and/or any subcontractor) must include [Federal Information Processing Standard (FIPS) 201-compliant](https://www.idmanagement.gov/approved-products-list%29) smart card readers (referred to as LACS Transparent Readers) with the purchase of servers, printers, desktops, and laptops.
2. **Mobile Devices**. The contractor must follow NIST 800-124, Rev. 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*and comply with Public Law 115-232 § 889*,* when purchasing mobile devices that process or store HHS data.

2.  Non-Commercial and Open-Source Computer Software Procurements

The Contractor (and/or any subcontractor) must follow secure coding best practice requirements, as directed by the United States Computer Emergency Readiness Team (US-CERT) specified standards and the Open Web Application Security Project (OWASP) that will limit system software vulnerability exploits. The contractor will be liable for malicious or defective code or failure to reduce risk.

3.  Information Technology Application Design, Development, or Support

1. The Contractor (and/or any subcontractor) must ensure IT applications designed and developed for end users (including mobile applications and software licenses) run in the standard user context without requiring elevated administrative privileges.
2. The contractor must consult the guidelines from NIST SP 800-160 volume 1, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, NIST SP 800-160 volume 2, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems***,**and NIST SP 800-53 to implement security during the development of all applications and throughout the life cycle stages of software development.
3. The Contractor (and/or any subcontractor) must follow secure coding best practice requirements, as directed by United States Computer Emergency Readiness Team (US-CERT) specified standards, the Open Web Application Security Project (OWASP), System Admin, Audit, Network and Security (SANS), and the *HHS Policy for Software Development Secure Coding Practices* that will limit system software vulnerability exploits.
4. The Contractor (and/or any subcontractor) must ensure that computer software developed on behalf of HHS or tailored from an open-source product, is fully functional and operates correctly on systems configured in accordance with government policy and federal configuration standards. The contractor must test applicable products and versions with all relevant and current updates and patches updated prior to installing in the HHS environment. No sensitive data must be used during software testing.
5. The contractor must, at a minimum, segregate physically or logically, all test and development systems from production systems as applicable in accordance with the HHS *Standard for Segregation of Dev/Test Environments from Production*.
6. The Contractor (and/or any subcontractor) must protect information that is deemed sensitive from unauthorized disclosure to persons, organizations or subcontractors who do not have a need to know the information. Information which, either alone or when compared with other reasonably available information, is deemed sensitive or proprietary by HHS must be protected as instructed in accordance with the magnitude of the loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. This language also applies to all subcontractors that are performing under this contract.

4.  Physical Access to Government Controlled Facilities

**(NOTE:** For procurements involving physical access to government facilities, selected language from Appendix B: Standards may apply. This includes, but not limited to security awareness, incident response, and HSPD-12. Consult with the ASPR Information Systems Security Officer (ISSO), ASPR Senior Official for Privacy (SOP) and other relevant stakeholders to select applicable language.)

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

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

Public Trust Clearance

Contractor personnel shall complete a background check and **Tier 2 Moderate Risk Public Trust clearance.**

.

*Draft Version 1.0/18 January 2023/BPA Call number one for MRC Website Services. /bw*