**Performance Work Statement (PWS)**

**for**

**Organ Procurement and Transplantation Network (OPTN) Next Generation (NextGen) Information Technology (IT)**

**Multiple Award Blanket Purchase Agreement (MA-BPA)**

January 14, 2025

[I. BACKGROUND 2](#_Toc187226487)

[II. PURPOSE 2](#_Toc187226488)

[III. SCOPE 2](#_Toc187226489)

[IV. PERIOD AND PLACE OF PERFORMANCE 3](#_Toc187226490)

[V. TASK AREAS 3](#_Toc187226491)

[Task Area 1: Software Development and Agile Teams 3](#_Toc187226492)

[Task Area 2: Product, User Research, and Design Support 5](#_Toc187226493)

[Task Area 3: Integration Services 6](#_Toc187226494)

[Task Area 4: Critical Infrastructure Protection and Information Assurance 7](#_Toc187226495)

[Task Area 5: IT Operations and Maintenance 7](#_Toc187226496)

[Task Area 6: IT Management Services 8](#_Toc187226497)

[Task Area 7: Coordination Among All Entities Supporting the OPTN 9](#_Toc187226498)

[Task Area 8: Transition Activities 10](#_Toc187226499)

[Task Area 9: General Requirements 11](#_Toc187226500)

[9.1 Branding, Media, and Reporting 11](#_Toc187226501)

[9.2 Use of Plain Language Guidelines and Other Government Laws and Regulations for all Products 11](#_Toc187226502)

[9.3 Contractor Non-Disclosure Agreement 12](#_Toc187226503)

[Task Area 10: Records Management Requirements 13](#_Toc187226504)

[Task Area 11: HHS Policy for Information Technology Procurements - Security and Privacy Language 14](#_Toc187226505)

[Task Area 12: Capital Planning and Investment Control and Earned Value Management 36](#_Toc187226506)

[Task Area 13: Enterprise Project Life Cycle (EPLC) 37](#_Toc187226507)

[Task Area 14: Personnel Security Requirements 37](#_Toc187226508)

[VI. Deliverables 40](#_Toc187226509)

[VII. Appendices 48](#_Toc187226510)

# BACKGROUND

Health Resources and Services Administration (HRSA), an agency of the U.S. Department of Health and Human Services (HHS), oversees the Organ Procurement and Transplantation Network (OPTN), as authorized by the National Organ Transplant Act of 1984 (42 USC 273 *et seq.*) and recently amended by Public Law 118-14. (Also see 42 CFR part 121). In March 2023, HRSA launched the [HRSA Organ Procurement and Transplantation Network Modernization Initiative](https://www.hrsa.gov/optn-modernization) to strengthen accountability and performance in the organ donation and transplantation system by focusing on critical areas such as improved technology, governance, and operations. The approach to improving technology will encompass a combination of off-the-shelf (OTS) solutions with some level of new development and/or customization(s) to optimize both time-to-value and ensure the overall solution meets the needs of HRSA and the OPTN while keeping patient safety paramount. The current system will be maintained under another contract.

The OPTN was established by Congress nearly four decades ago and consists of a comprehensive network of transplant professionals, community members, and others charged with increasing organ donation and operating and overseeing a fair and accountable system for allocating and transplanting organs in the United States. HRSA has worked to strengthen the OPTN to better meet the urgent needs of the more than 100,000 people on the organ transplant waitlist and their families.

# PURPOSE

HRSA has a need for a streamlined and common contracting vehicle to support the research, design, development, configuration, customization, and deployment of modern IT solutions to the OPTN system. The system facilitates the allocation and distribution of donor organs to individuals waiting for an organ transplant. OPTN computer system metrics can be found at <https://optn.transplant.hrsa.gov/data/dashboards-metrics/optn-computer-system-metrics/>. Once deployed, HRSA will have a need for ongoing enhancements and production support for solutions. While meeting the Modernization Initiative objectives and ensuring uninterrupted services for organ transplantation in the United States, HRSA requires access to expert services in the areas of product management, human-centered design (HCD), agile application development, Application Programming Interface (API) development, systems security, database management and security, accessibility and 508 Compliance, automated testing, cloud infrastructure design and management, continuous integration/continuous delivery (CI/CD), and/or Development, Security and Operations (DevSecOps) services.

# SCOPE

Using modern, human-centered design practices and delivery methodologies, the OPTN NextGen IT MA-BPA (hereinafter referred to as NextGen IT MA-BPA) includes the services necessary for research, design, development, testing, and piloting of modules leading to modernized, secure, and flexible OPTN software solutions and information technology. The contractor, acting as an independent contractor and not as an agent of the government, shall furnish all materials, personnel, facilities, support and management necessary to provide the services and solutions as set forth in the Scope of Work below.

# PERIOD AND PLACE OF PERFORMANCE

The base award will be for one, five-year ordering period. The work will be performed offsite at the Contractor’s location, unless specified otherwise at the task order level.

If the COR determines that laptops are needed by the contractor on a specific order, the Government will provide the Contractor a number of laptops as specified in the order award.

HRSA provides Dell Latitude (or replacement model) as a standard laptop for Contractors HRSA will also provide any offsite Contractors with the necessary remote network access to perform this requirement. HRSA will also be responsible for ensuring the necessary software licenses are provided to conduct work. In the event of emergency weather conditions or when the Federal Government is closed on days other than specified in this contract, Contractor shall perform work at their offsite office premises.

# TASK AREAS

This MA-BPA encompasses services in support of OPTN Modernization Initiative technology solutions. This includes the incorporation of Agile methodologies and ceremonies into work, such as (but not limited to) sprint planning, daily scrum, sprint review, sprint retrospective, backlog grooming, and estimating activities. Where applicable, a Human Centered Design approach that actively involve users in the design and development of solutions will be incorporated. This includes incorporating best practices for user research and usability testing, such as (but not limited to) creating user personas, defining the problem space, developing affinity maps, designing user flow diagrams, wireframes, information architecture diagrams, prototypes and comprehensive user research plans.

### Task Area 1: Software Development and Agile Teams

The objective of this task area is to develop customized software applications, database applications, and provide access to agile teaming arrangements for a variety of OPTN IT systems and Modernization Initiative efforts. Work in this task area includes performing deep dive research and discovery on existing processes and OPTN technologies, defining technology architecture that will enable industry standard or better ease of performance, refactoring of legacy systems, navigating code with complex interdependencies to break out business logic and decrease risks, evaluation and testing of products, creation of automated testing suites, collaborative and cross-functional implementation, and management of agile teaming arrangements.

Specific technologies to be used (if known) will be communicated at the Task Order level but will commonly include industry-standard web programming languages and frameworks such as JavaScript, Ruby, Java, and .NET; or Commercial Off-The-Shelf (COTS) products and platforms that can be used or adapted to meet HRSA’s OPTN needs. Specific capabilities to be delivered by a team will be defined at the Task Order level and may include (but are not limited to) developing/modifying responsive web applications, developing/modifying REST APIs, and developing/modifying native mobile applications. Activities may include (but are not limited to) writing custom software, configuring Software as a Service (SaaS) platforms, or configuring COTS products to support specific objectives. This includes procurement of small quantities of non-production licenses for discovery and prototyping. Software developed under this MA-BPA shall be covered by automated unit and integration tests, and all software and configurations created under the MA-BPA shall be developed in a modern software version control system specified by HRSA at the order level. Contractors shall use both code reviews and automated checks to ensure software quality. The Contractor shall monitor industry trends and propose suitable technologies to HRSA to implement requested functionality. The Contractor shall incorporate Agile methodologies and ceremonies such as (but not limited to) sprint planning, daily scrum, sprint review, sprint retrospective, backlog grooming, and estimating activities as part of this work.

A comprehensive, but not limited, sampling of work to be performed under this task area is shown below:

1. Discovery
2. Engineering
3. Refactoring of Legacy Systems
4. Usability Testing
5. Data Science and Analytics
6. Deployment
7. Security and Operations (DevSecOps)
8. Automated Testing Suite
9. User Research and Design
10. Agile Teaming
11. Project Metrics Reporting and Analytics
12. Standards Development for Health IT Services
13. Business Intelligence
14. Web Development and Support
15. IT Strategic Planning
16. Requirements Analysis, Design, Coding, and Testing
17. Application Prototyping
18. Multimedia Software for Patient/Staff Education
19. Program Evaluation Software
20. Administrative and General Decision Support Software
21. Business Intelligence and Analytics
22. GIS-Enhanced Planning and Program Evaluation Software
23. Web 2.0 Development and Management
24. Database Development and Management
25. Clinical Protocol and Quality Assurance Decision Support Software
26. Customer Support

### Task Area 2: Product, User Research, and Design Support

The objective of this task area is to provide the support for the product management lifecycle and human-centered design process. This includes leveraging a range of qualitative and quantitative user research methods to determine people’s goals, needs, and behaviors to

develop user personas to drive product strategy, requirements, and metrics of success. It involves synthesizing user research and usability testing to create a product roadmap to drive a technical strategy. Product road-mapping incorporates an iterative, phased approach to continuously re-assess product direction and prioritization based on user feedback and data.

Specific technologies to be used (if known) will be communicated at the Task Order level but will commonly include industry-standard product management and design tools such a Jira, Confluence, Figma, Mural, Miro etc. Specific capabilities to be delivered by a team will be defined at the Task Order level and may include (but are not limited to) product requirement documentation, project management and project status updates, wireframes, service designs, prototypes and other diagrams/visuals, interview guides, research briefs, and training materials. The Contractor shall incorporate Agile methodologies and ceremonies such as (but not limited to) sprint planning, daily scrum, sprint review, sprint retrospective, backlog grooming, and estimating activities as part of this work.

A comprehensive, but not limited, sampling of work to be performed under this task area is shown below:

1. Discovery
2. User Research including engagement plans and interview guides
3. User research analyses and recommendations
4. Project Management
5. Product Road-mapping and Prioritization
6. Product Strategy
7. Product Definition, Scoping, and Requirements
8. Identifying and defining Key Success Metrics
9. Metrics Tracking, Reporting, and Analytics
10. Human-Centered Design
11. Plain-Language Content Writing
12. Usability Testing
13. Cross-Functional Collaboration
14. Go-to-market planning and launch support
15. Prototyping
16. Inclusive Design/Accessibility/Section 508 Compliance
17. Wireframing
18. Service blueprints
19. Information Architecture Design
20. Training materials (i.e. Customer Support Manual, Statement of Processes Documentation)
21. Workflow design

### Task Area 3: Integration Services

The objective of this task area is to support the development and deployment of integrated information systems, which includes the integration of technical components, information technology components, organizational components and documentation. The Contractor shall integrate open source, COTS, Government Off the Shelf (GOTS) and/or SaaS solutions into existing, custom built, or new systems and provide configuration, customization and implementation services. The Contractor shall also integrate with other government systems using modern standards-based communication protocols and data formats. The Contractor shall incorporate Agile methodologies and ceremonies such as (but not limited to) sprint planning, daily scrum, sprint review, sprint retrospective, backlog grooming, and estimating activities as part of this work.

A comprehensive, but not limited, sampling of work to be performed under this task area is shown below:

1. Infrastructure Engineering, Development, Implementation, Integration
2. Enterprise Application Integration
3. Gap Analysis and Benchmarking
4. Integration of Health Systems Across Federal Agencies and Public and Private Healthcare Systems, such as Epic, Cerner.
5. Data Migration and Integration
6. Open Source Integration
7. Enterprise Data Management
8. Collaboration Tools
9. Business Process Reengineering
10. Test and Evaluation Services
11. Financial Analysis
12. Feasibility Studies
13. Requirements Analysis
14. System Design Alternative (SDA) Studies
15. Systems Engineering
16. Architecture Validation and Verification
17. Risk Assessment
18. Hardware Integrations

### Task Area 4: Critical Infrastructure Protection and Information Assurance

The objective of this task area is to support the protection of critical infrastructure, assurance of agency information, and operations that protect and defend information and information systems by ensuring confidentiality, integrity, availability, accountability, restoration, authentication, non- repudiation, protection, detection, monitoring, and event react capabilities. The Contractor shall incorporate Agile methodologies and ceremonies such as (but not limited to) sprint planning, daily scrum, sprint review, sprint retrospective, backlog grooming, and estimating activities as part of this work.

A comprehensive, but not limited, sampling of work to be performed under

this task area is shown below:

1. Cyber Security
2. Information Assurance of Critical Infrastructure
3. Risk Management (Vulnerability Assessment and Threat Identification)
4. Information Systems Security
5. Application Security
6. Disaster Recovery
7. Incident Response Planning and Execution
8. Security Certification and Accreditation
9. Federal Information Security Modernization Act (FISMA) Implementation Support
10. Health Insurance Portability and Accountability Act Implementation Support
11. Record Management

### Task Area 5: IT Operations and Maintenance

The objective of this task area is to support the operation and maintenance of IT systems, keeping IT systems viable with supported vendor releases or off-the-shelf applications software upgrades. Operations and maintenance on IT systems shall include all software and hardware associated with mainframes, client/server, web-based applications, and networking. These services maybe provided on Government sites and/or at Contractors facilities. The Contractor shall incorporate Agile methodologies and ceremonies such as (but not limited to) sprint planning, daily scrum, sprint review, sprint retrospective, backlog grooming, and estimating activities as part of this work.

A comprehensive, but not limited, sampling of work to be performed under this task area is shown below:

1. Operational Support
2. Software Maintenance and Upgrades
3. Telecommunications Maintenance (Data, Voice, Images, including Wireless)
4. Infrastructure Management Services (IMS)
5. Configuration Management
6. Network/Hardware Support
7. Resource Management
8. Backup and Recovery Management
9. Installation, Configuration, and Tuning
10. Electronic Software Licensing Services including license: deployment, management, tracking, upgrading, etc.
11. System Management
12. IT Training and Coaching
13. IT Operation and Maintenance Planning
14. Data Quality Management
15. Transformation Services
16. Continual Service Improvement
17. Balanced Scorecard for Operations
18. IT Infrastructure Optimization

### Task Area 6: IT Management Services

The objective of this task area is to provide the Information Technology (IT) infrastructure and IT services required to assume management and operations of government IT resources and IT business functions. The Contractor shall incorporate Agile methodologies and ceremonies such as (but not limited to) sprint planning, daily scrum, sprint review, sprint retrospective, backlog grooming, and estimating activities as part of this work.

A comprehensive, but not limited, sampling of work to be performed under

this task area is shown below:

1. Program Management
2. Program Management Office Support
3. IT Service Management
4. IT Portfolio Analysis
5. Risk Management
6. Capital Planning and Investment Control Support
7. Help Desk/IT Support
8. Management of Call Centers
9. Network Operations and Web Management Support
10. Leasing of Hardware and Software
11. Tools and Applications (including Application Service Provider)
12. Hardware/Software Maintenance
13. Transition Planning
14. Data Base Administration and Data Storage Management
15. Production Control and Management
16. Asset Management (including Radio Frequency Identification [RFID] Tracking)
17. Managed IT Services Support
18. IT Impact Analyses
19. Workflow Management
20. Implementation of Standards (e.g., International Organization for Standardization
21. (ISO) 9000, Capability Maturity Model Integration (CMMI), IT Services Management)
22. Solution Leasing
23. Software-as-a-service
24. Accessibility Services (508 and 504 compliance)

### Task Area 7: Coordination Among All Entities Supporting the OPTN

This task area encompasses work and requirements to cooperate and collaborate with all entities supporting the OPTN. Entities supporting the OPTN includes HRSA, other contractors, and other Federal agencies.

The Contractor shall:

1. Meet with other entities supporting the OPTN on a regular basis to be determined by HRSA to report on the status of deliverables and action items and shared metrics, conduct strategic planning, collaborate on innovative reforms, identify and address risks, and coordinate with other contractors to implement the HRSA OPTN Modernization Initiative.
2. Enter into data use agreements for OPTN data with other entities contracted to support the OPTN, as necessary and at the direction of HRSA.
   1. Implement all appropriate privacy and security protections for OPTN-related materials, as referenced other task areas and future task orders.
   2. Share all data and information necessary to enable OPTN and all entities supporting the OPTN to successfully perform. This includes assisting with access to OPTN data, process and procedure documentation, and other data necessary to complete OPTN activities. NOTE: Any potential restrictions on the part of contractors to sharing data and necessary information must be identified at the time of task order request.
3. Report to HRSA all data, information, and other requested OPTN-related materials to support HRSA’s oversight and congressional, statutory, regulatory, financial and other reporting requirements and oversight function.
4. Continually monitor, manage, and adjust processes, procedures, and functionality to integrate work with other entities supporting the OPTN.
5. Continually monitor, identify, and mitigate risks and proactively inform HRSA of any issues that prevent performance or successful implementation of efforts.
6. Conduct and participate in retrospectives to work collaboratively with other entities supporting the OPTN to identify issues and achievements, develop recommendations for improvement, and report on outcomes.
7. Incorporate Agile methodologies and ceremonies such as (but not limited to) sprint planning, daily scrum, sprint review, sprint retrospective, backlog grooming, and estimating activities as part of this work.

### Task Area 8: Transition Activities

This task area encompasses services required to enable the transition of any contract activities from incumbent contractors to other entities, including HRSA, the OPTN, HRSA contractors, and other entities supporting the OPTN. This includes both transition-in at the start of performance and transition-out at the end of performance. The Contractor shall incorporate Agile methodologies and ceremonies such as (but not limited to) sprint planning, daily scrum, sprint review, sprint retrospective, backlog grooming, and estimating activities as part of this work.

At the direction of the COR, the Contractor shall:

1. Develop a transition plan for HRSA review and approval outlining the details of any transition (including applicable implementation roadmaps, risk management, privacy, back-up protocols, document transfer and processes) and implement approved plans to ensure successful transition.
2. Coordinate and implement the transition of any existing function or activity (including but not limited to processes, protocols, data collection or analyses, templates, systems) in such a way that ensures users have a seamless experience. This may include collaboration, coordinating, and training for multiple entities supporting the OPTN.

### Task Area 9: General Requirements

#### 9.1 Branding, Media, and Reporting

##### 9.1.1 Branding

Contractors shall brand all OPTN products produced under contracts associated with this MA-BPA as OPTN products. OPTN products can only contain OPTN branding. Contractors shall not brand any OPTN product as a product of the entity supporting the OPTN or as joint OPTN products. No contractor shall brand any product not produced or approved to support the OPTN as an OPTN product. Additionally, contractors will ensure a consistent look, feel, and voice across all user-facing sites and services, as directed by HRSA.

##### 9.1.2 Media Inquiries and Public Release of Information

Contractors must work through the COR to obtain HRSA review and approval of any responses to the media or before putting any information related to performance under this contract out publicly.

##### 9.1.3 Reporting

Contractors shall contribute to the development of internal and external reports as necessary for HRSA to meet statutory and regulatory requirements, including information such as data and analyses on organ donation and transplantation, policies and policy development, and system activities.

#### 9.2 Use of Plain Language Guidelines and Other Government Laws and Regulations for all Products

The Contractor shall:

1. Follow the federal Plain Language Guidelines when developing products. The Plain Language Act of 2010 requires federal agencies to create communications that are clear and understandable to the public.
2. Produce content that follows [federal plain language guidelines](https://www.plainlanguage.gov/guidelines/). All text content must aim for a [Flesch-Kinkaid Reading Ease](https://readable.com/readability/flesch-reading-ease-flesch-kincaid-grade-level/) score of at least 60. HRSA’s Office of Communications’ liaisons use [Readable](https://readable.com/) to review, update, and score content. Contractor shall work with the Contracting Officer’s Representative (COR) and program communications liaisons and use Readable to review, score and enhance the content.
3. Use PlainLanguage.gov’s [Checklist for Plain Language](https://www.plainlanguage.gov/resources/checklists/checklist/) and [HHS’s Plain Writing Checklist](https://www.hhs.gov/web/building-and-managing-websites/managing-websites/plain-writing-in-one-page/index.html) as guidelines.
4. Ensure that all materials adhere to federal copyright laws including the citation of sources in endnotes or footnotes; obtaining written permission to reproduce, reprint, or adapt existing materials used in the creation of materials under this contract; and including credits for images, which include photographs, pictures, illustrations, tables, charts, figures, and graphs.
5. Ensure that all materials adhere to the Government Printing and Binding Regulations, including the prohibition on commercial advertising which says, “No Government publication or other Government printed matter, prepared or produced with either appropriated or nonappropriated funds or identified with an activity of the Government, shall contain any advertisement inserted by or for any private individual, firm, or corporation; or contain material which implies in any manner that the Government endorses or favors any specific commercial product, commodity, or service.” -- (Title III--General Provisions, 13. Advertisements, Commercial.)
6. Ensure that all materials do not contain any non-federal logos (since logos are a form of institutional advertising); that materials do not contain contact information for non-federal organizations, except the website address for informational purposes; and that all materials do not contain any contact information for individuals.
7. Ensure that all materials do not contain the name of the contractor or subcontractors since this is also a form of advertising.
8. Ensure that all materials adhere to the prohibition against referring to lobbying in materials produced with appropriated funds. The prohibition against lobbying also includes grassroots lobbying, which is advocating for a change in legislation at the federal, state, or community level.

#### 9.3 Contractor Non-Disclosure Agreement

The Contractor shall:

1. Complete and submit the Information Technology System Contractor Non-Disclosure Agreement (NDA) (see Appendix A) for all personnel requiring access to sensitive information, including but not limited to Personally Identifiable Information (PII), non-public information, confidential information, or Uncontrolled Classified Information (UCI) from the files of the Department of Health and Human Services (HHS) under this contract.
   1. Requirements:
      1. Completion of NDA: Each individual must fully execute the NDA prior to accessing any sensitive information.
      2. Submission: The completed NDA must be submitted to the Contracting Officer’s Representative (COR) for review and approval.
      3. Access Restriction: Personnel will not be granted access to sensitive information until the COR provides written approval of the submitted NDA.
      4. Retention: A copy of the approved NDA will be retained by the COR and contractor for audit and compliance purposes.

Failure to comply with this requirement will result in immediate suspension of access privileges and may lead to further contractual or administrative action.

### Task Area 10: Records Management Requirements

1. Records and Information Regulations Guidelines

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

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

1. Records and Information Management

The Contractor shall manage and maintain Federal records and/or information, including electronic records and/or information, ensuing from this contract in accordance with all applicable records management laws and regulations, including but not limited to the Federal Records Act (44 U.S.C. Chapters. 21, 29, 31, 33); 36 CFR § 1236.20 What are appropriate record keeping systems for electronic records? & 1236.22 What are the additional requirements for managing electronic mail records? (<http://www.ecfr.gov/cgi-bin/text-> idx?rgn=div5&node=36:3.0.10.2.25); [NARA Bulletin 2013-02, August 29, 2013, Guidance on a](http://www.ecfr.gov/cgi-bin/text-idx?rgn=div5&node=36%3A3.0.10.2.25) [New Approach to Managing Email](http://www.ecfr.gov/cgi-bin/text-idx?rgn=div5&node=36%3A3.0.10.2.25) Records ([https://www.archives.gov/records-](http://www.archives.gov/records-) mgmt/bulletins/2013/2013-02.html); and NARA [Bulletin 2010-05 September 08, 2010](https://www.archives.gov/records-mgmt/bulletins/2013/2013-02.html) [(http://www.archives.gov/records-mgmt/bulletins/2010/2010-05.html)](http://www.archives.gov/records-mgmt/bulletins/2010/2010-05.html), Guidance on Managing Records in Cloud Computing Environments.

Managing the records includes, maintaining records to retain functionality and integrity throughout the records' full lifecycle including: (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.

1. Records Management Training
2. The contractor (and/or subcontractor) shall ensure that all employees having access to (1) Federal information or a Federal information system, or (2) personally identifiable information (PII), complete the HHS Records Management Training before performing work under this contract, and thereafter completing the annual refresher course during the life of the contract. The training is located at <https://humancapital.learning.hhs.gov/courses/2022recordsmanagement/01_index.html>. At the end of the Records Management training, the “Congratulations" slide is considered your certificate of completion. Please send the completion certificates to the Contracting Officer Representative (COR) of the contract. The listing of completed training shall be included in the first progress report. Any revisions to this listing as a result of staffing changes shall be submitted with next required progress report.

Deliverable: Provide Records Management training completion certificates – Due Date: within 30 days after contract award and upon new staff onboarding and thereafter completing the annual refresher course during the life of the contract.

### Task Area 11: HHS Policy for Information Technology Procurements - Security and Privacy Language

I. Procurements Requiring Information Security and/or Physical Access Security

1. Baseline Security Requirements
   1. **Applicability.**The requirements herein apply whether the entire contract or modification (hereafter "contract"), or portion thereof, includes either or both of the following:
      1. **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.
      2. **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.
   2. **Safeguarding Information and Information Systems.** All government information and information systems must be protected in accordance with HHS/HRSA policies and level of risk. At a minimum, the Contractor (and/or any subcontractor) must:
      1. 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.  
             
           ***Note to the Requiring Activity Representative:****Complete the following section using the information obtained from the Information Security and Privacy Certification Checklist.*
      2. Categorize all information owned and/or collected/managed on behalf of HHS/HRSA 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, HRSA Senior Official for Privacy (SOP), or other representative, the impact level for each Security Objective (Confidentiality, Integrity, and Availability) and the Overall Impact Level, which is the highest watermark of the three factors of the information or information system are the following:
         * **Confidentiality:** [  ] Low [ X ] Moderate [  ] High
         * **Integrity:** [  ] Low [  ] Moderate [ X ] High
         * **Availability:**[  ] Low [ X ] Moderate [  ] High
         * **Overall Impact Level:**[  ] Low [  ] Moderate [ X ] High
      3. 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/HRSAregardless of location or purpose.
      4. 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).
      5. Adopt and implement all applicable policies, procedures, controls, and standards required by the HHS/HRSA 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/HRSA security and/or privacy officials.
   3. **Privacy Act.** Comply with the Privacy Act requirements (when applicable), and tailor FAR and HHSAR clauses as needed.
   4. **Privacy Compliance.** Comply with the E-Government Act of 2002, NIST SP 800-53, and applicable HHS/OpDiv privacy policies, and complete all the requirements below:  
        
      ***Note to the Requiring Activity Representative:****This information may be included after award in the event it is not yet available at the time of acquisition. Section d must be included in all contracts regardless of whether or not personally identifiable information (PII) is involved.*
      1. 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.
      2. 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.
      3. The Contractor must support the agency with conducting a Privacy Threshold Analysis (PTA) for the information system and/or information handled under this contract to determine whether or not PII is collected, disseminated, maintained, or disposed as part of the contract. The PTA will determine if a full Privacy Impact Assessment (PIA) needs to be completed.
         * If the results of the PTA show that a full PIA is needed, the Contractor must support the agency with completing a PIA for the system or information within 60 days after completion of the PTA and in accordance with HHS policy and OMB M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*.
         * The Contractor must support the agency in reviewing the PIA at least every ***three years*** throughout the system development lifecycle (SDLC)/information lifecycle, or when determined by the agency that a review is required based on a major change to the system, or when new types of PII are collected that introduces new or increased privacy risks, whichever comes first.
   5. **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:
      1. Marked appropriately;
      2. Disclosed to authorized personnel on a Need-To-Know basis;
      3. 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
      4. 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*.
   6. **Protection of Sensitive Information**. For security purposes, information is *or*may be sensitive because it requires security to protect its confidentiality, integrity, and/or availability. The Contractor (and/or any subcontractor) must protect all government information that is or may be sensitive by securing it with a solution that is validated with current FIPS 140 validation certificate from the NIST CMVP.
   7. **Confidentiality and Nondisclosure of Information**. Any information provided to the contractor (and/or any subcontractor) by HHS or collected by the contractor on behalf of HHS 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 HRSA policies. Unauthorized disclosure of information will be subject to the HHS/HRSA sanction policies and/or governed by the following laws and regulations:
      1. 18 U.S.C. 641 (Criminal Code: Public Money, Property or Records);
      2. 18 U.S.C. 1905 (Criminal Code: Disclosure of Confidential Information); and
      3. 44 U.S.C. Chapter 35, Subchapter I (Paperwork Reduction Act).
   8. **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)*.
   9. **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.
   10. **Government Websites.** All new and existing public-facing government websites must be securely configured with Hypertext Transfer Protocol Secure (HTTPS) using the most recent version of Transport Layer Security (TLS). In addition, HTTPS must enable HTTP Strict Transport Security (HSTS) to instruct compliant browsers to assume HTTPS at all times to reduce the number of insecure redirects and protect against attacks that attempt to downgrade connections to plain HTTP. For internal-facing websites, HTTPS is not required, but it is highly recommended. Consult the *HHS Policy for Internet and Email Security* for additional information.
   11. **Contract Documentation**. The Contractor must use provided templates, policies, forms and other agency documents to comply with contract deliverables as appropriate.
   12. **Standard for Encryption.**The Contractor (and/or any subcontractor) must:
       1. Comply with the *HHS Standard for Encryption of Computing Devices and Information*to prevent unauthorized access to government information.
       2. Encrypt all sensitive federal data and information (i.e., PII, protected health information [PHI], proprietary information, etc.) in transit (i.e., email, network connections, etc.) and at rest (i.e., servers, storage devices, mobile devices, backup media, etc.) with encryption solution that is validated with current FIPS 140 validation certificate from the NIST CMVP.
       3. Secure all devices (i.e.: desktops, laptops, mobile devices, etc.) that store and process government information and ensure devices meet HHS and HRSA-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).
       4. Verify that the encryption solutions in use have been validated under the Cryptographic Module Validation Program to confirm compliance with current FIPS 140 validation certificate from the NIST CMVP. The Contractor must provide a written copy of the validation documentation to the COR.
       5. 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.
   13. **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 HRSA non-disclosure agreement. Contractors (and/or subcontractors) must submit a copy of each signed and witnessed NDA to the Contracting Officer (CO) and/or CO Representative (COR) prior to performing any work under this acquisition.
2. Training Requirements
   1. **Mandatory Training for All Contractor Staff.** All Contractor (and/or any subcontractor) employees assigned to work on this contract and have access to HRSA’s network must complete the applicable *HHS/HRSA Cybersecurity Awareness Training* training (provided upon contract award) before performing any work under this contract. Thereafter, the employees must complete *HHS/HRSA Cybersecurity Awareness Training* at least ***annually***, during the life of this contract. All provided training must be compliant with HHS training policies.
   2. **Role-based Training.** All Contractor (and/or any subcontractor) employees with significant security responsibilities (as determined by the program manager) must complete *Role-Based Training for IT Admin* ***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.
   3. **Training Records.** The Contractor (and/or any subcontractor) must maintain training records for all its employees working under this contract in accordance with HHS policy. A copy of the training records must be provided to the CO and/or COR within ***30 days*** after contract award and ***annually*** thereafter or upon request.
3. Rules of Behavior
   1. The Contractor (and/or any subcontractor) shall ensure that all employees performing on the contract comply with the *HHS Information Technology General Rules of Behavior* (included in the *HHS/HRSA Cybersecurity Awareness Training*), and any applicable system-level rules of behavior.
   2. All Contractor employees performing on the contract must read and adhere to the Rules of Behavior before accessing Department data or other information, systems, and/or networks that store/process government information, initially at the beginning of the contract and at least ***annually*** thereafter, which may be done as part of annual *HHS/HRSA Cybersecurity Awareness Training*. If the training is provided by the contractor, the signed ROB must be provided as a separate deliverable to the CO and/or COR per defined timelines above.
4. Incident Response
   1. The Contractor (and/or any subcontractor) must respond to all alerts/Indicators of Compromise (IOCs) provided by HHS Computer Security Incident Response Center (CSIRC)/HRSA Computer Security Incident Response Team ([hrsacsirt@hrsa.gov](mailto:hrsacsirt@hrsa.gov)) **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)*."
   2. In the event of a suspected or confirmed incident or breach, the Contractor (and/or any subcontractor) must:
      1. Protect all sensitive information, including any PII created, stored, or transmitted in the performance of this contract, with encryption solution that is validated with current FIPS 140 validation certificate from the NIST CMVP.
      2. 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 HRSA approved notifications to affected individuals following specific instructions from the HHS Privacy Incident Response Team (PIRT).
      3. Report all suspected and confirmed information security and privacy incidents and breaches to the HRSA Computer Security Incident Response Team ([hrsacsirt@hrsa.gov](mailto:hrsacsirt@hrsa.gov)) or 301-443-3333, COR, CO, HRSA 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 HRSA 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.
      4. Comply with OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information,* and HHS and HRSA privacy breach response policies when handling PII breaches.
      5. Provide full access and cooperate on all activities as determined by the Government to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents. This may involve disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls. This may also involve physical access to contractor facilities during a breach/incident investigation.
5. Position Sensitivity Designations  
   All Contractor (and/or any subcontractor) employees must obtain a background investigation commensurate with their position sensitivity designation that complies with Parts 1400 and 731 of Title 5, Code of Federal Regulations (CFR). The following position sensitivity designation levels apply to this solicitation/contract:

* non sensitive, moderate risk public trust Tier 2 investigation
* non sensitive, high risk public trust Tier 4 investigation (this level applies when elevated rights are needed for system access.)

1. Homeland Security Presidential Directive (HSPD)-12  
     
   The Contractor (and/or any subcontractor) and its employees must comply with Homeland Security Presidential Directive (HSPD)-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*; OMB M-05-24; OMB M-19-17; FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*; HHS HSPD-12 policy; and*Executive Order 13467, Part 1 §1.2.*  
     
   ***Note to the Requiring Activity Representative:****For additional information, see HSPD-12 policy at:*<https://www.dhs.gov/homeland-security-presidential-directive-12>)
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, have the ability to access, or host and/or maintain a government information system(s). The roster must be submitted to the COR and/or CO within 14 days of the effective date of this contract. Any revisions to the roster as a result of staffing changes must be submitted within 14 days of the change. The COR will notify the Contractor of the appropriate level of investigation required for each staff member.   
     
   If the employee is filling a new position, the Contractor must provide a position description and the Government will determine the appropriate suitability level.
3. Contract Initiation and Expiration
   1. **General Security Requirements.** The Contractor (and/or any subcontractor) must comply with information security and privacy requirements, Enterprise Performance Life Cycle (EPLC) processes, HHS Enterprise Architecture requirements to ensure information is appropriately protected from initiation to expiration of the contract. All information systems development or enhancement tasks supported by the contractor must follow the HHS EPLC framework and methodology and in accordance with the HHS Contract Closeout Guide (2012).
   2. **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.
   3. **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, including HRSA Disposition Planto the CO and/or COR to certify that, at the government's direction, all electronic and paper records are appropriately disposed of and all devices and media are sanitized in accordance with NIST SP 800-88, *Guidelines for Media Sanitization*.
   4. **Notification.** The Contractor (and/or any subcontractor) must notify the CO and/or COR and system ISSO within 14 days before an employee stops working under this contract.
   5. **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 HRSA policies.
   6. The Contractor (and/or any subcontractor) must perform and document the actions identified in the HRSA Clearance Form for Separating Employees and Contractors (Form-419) when an employee terminates work under this contract within 14 days of the employee's exit from the contract. All documentation must be available to the CO and/or COR upon request.
4. Records Management and Retention
   1. 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 HRSA policies and must not dispose of any records unless authorized by HHS*/*HRSA.
   2. In the event that a contractor (and/or any subcontractor) accidentally disposes of or destroys a record without proper authorization, he/she must document and report the incident in accordance with HHS*/*HRSA policies.
5. High Value Asset (HVA)  
     
   If a system is identified as HVA, the contractor must comply with the HHS Policy for the High Value Asset (HVA) Program and the [DHS HVA Control Overlay](https://www.cisa.gov/publication/high-value-asset-control-overlay) in addition to the above requirements.

**II.  Requirements for Procurements Involving Privacy Act Records**

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 particular.

The System of Records Notice that is applicable to this contract is: 09-15-0055, Organ Procurement and Transplantation Network (OPTN)/Scientific Registry of Transplant Recipients (SRTR) Data System, HHS/HRSA/HSB/DoT. (<https://www.federalregister.gov/documents/2022/08/01/2022-16344/privacy-act-of-1974-system-of-records>).

**III. Procurements Involving Government Information Processed on GOCO or COCO Systems**

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)*, *HRSA Information Security Policy*; *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. The Contractor must conduct the A&A requirements in accordance with *HHS IS2P/HRSA Information Security Policy*, NIST SP 800-37, *Guide for Applying the Risk Management Framework to Information Systems: A Security Life Cycle Approach*(latest revision), NIST SP 800-53B, *Control Baselines for Information Systems and Organizations*, and the NIST SP 800-53A (latest revision).  
        
      ***Note to the Requiring Activity Representative:****For an existing ATO, the OpDiv 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.*  
        
      *HRSA’s* 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. An A&A package must contain the following documentation. Following the initial ATO, the Contractor must review and maintain the ATO in accordance with HHS*/*HRSA policies*.* The Contractor (and/or any subcontractor) must provide an A&A package at least 30 days prior to the ORR to the CO and/or COR. Additional information on each of the listed document requirements can be found in [System Security Requirements and Guidance.pdf]. The following A&A deliverables are required to complete the A&A package:
         * E‐Authentication (E‐Auth) Risk Assessment Questionnaire
         * Privacy Threshold Analysis (PTA)
         * Privacy Impact Assessment (PIA), if applicable
         * System of Records Notice (SORN), if applicable
         * Risk Assessment Report
         * Business Impact Analysis (BIA)
         * Contingency Plan (CP)
         * Contingency Plan Test Plan and Test Report
         * System Interconnection Agreements
         * Security Configurations
         * Configuration Management Plan
         * Incident Response Plan, if applicable
         * System Security Plan (SSP)
         * Security Assessment Report (SAR)
         * Plan of Action and Milestones (POA&M)
         * Continuous Monitoring Plan, if applicable
      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 Security Control Assessment** - 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. In addition, review all relevant A&A documentation (SSP, POA&M, Contingency Plan, etc.) and provide updates by specified due date.
      4. **Penetration Test** – Applicable to HVA and Systems categorized as High. Involves penetration testing conducted by the agency or independent third-party.
      5. **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 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.
      6. **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*/HRSA* at least monthly and 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.
      7. **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 weekly and upon request.
      8. **Patching and Vulnerability Remediation -** All vulnerabilities and findings must be remediated, in accordance with timelines based on their residual risk as specified in the HHS POA&M Standard and HHS Policy for Vulnerability Management:
         * 15 days from discovery date for Critical risk vulnerabilities
           + Critical vulnerabilities require remediation prior to release into Production.
         * 30 days from discovery date for High risk vulnerabilities
           + High vulnerabilities require remediation prior to release into Production.
         * 90 days from discovery date for Moderate risk vulnerabilities
         * 365 days from discovery date for Low risk vulnerabilities

The HRSA VM team and the ISSO will determine the risk rating of vulnerabilities. The HRSA CISO may direct out of band patching due to potential active exploit, zero day vulnerability, etc.

* + 1. **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. Code and Application Scans provided prior to all new releases.
    2. **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).
  1. **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.
  2. **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 HRSA CISO if it impacts only HRSA). 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*.
  3. **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 certificate from the NIST CMVP.
     2. Configure laptops and desktops in accordance with HRSA Secure Configuration Baselines and HHS Minimum Security Configuration Standards;
     3. Maintain the latest operating system patch release and anti-virus software definitions;
     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 on a monthly basis and report the results of these scans to the CO and/or COR, Project Officer, and any other applicable designated POC.
  4. **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.
  5. **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.

**IV.  Contracts Involving Cloud Services**

1. HHS FedRAMP Privacy and Security Requirements  
     
   The Contractor (and/or any subcontractor) must be responsible for the following privacy and security requirements:
   1. **FedRAMP Compliant ATO**. Comply with FedRAMP Assessment and Authorization (A&A) requirements and ensure the information system/service under this contract has a valid FedRAMP compliant (approved) authority to operate (ATO) in accordance with Federal Information Processing Standard (FIPS) Publication 199 defined security categorization. If a FedRAMP compliant ATO has not been granted, the Contractor must submit a plan to obtain a FedRAMP compliant ATO.
      1. Implement applicable FedRAMP baseline controls commensurate with the agency-defined security categorization and the applicable FedRAMP 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 (FedRAMP) 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 FedRAMP 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 FedRAMP 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.
   3. **Service Level Agreements.** *Add when applicable* The Contractor must understand the terms of the service agreements that define the legal relationships between cloud customers and cloud providers and work with HRSA to develop and maintain an SLA.
   4. **Interconnection Agreements/Memorandum of Agreements.***Add when applicable* The Contractor must establish and maintain Interconnection Agreements and or Memorandum of Agreements/Understanding in accordance with HHS/HRSApolicies.
2. 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*/*HRSA 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 FedRAMP 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/HRSA. 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.
3. Assessment and Authorization (A&A) Process
   1. The Contractor (and/or any subcontractor) must comply with HHS and FedRAMP 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*/*HRSA security policies.
      1. In addition to the FedRAMP 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 HRSA 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 FedRAMP accredited third-party assessment organization (3PAO); moderate impact CSP systems must make a best effort to use a FedRAMP 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 documentation, where applicable. Following the initial ATO, the Contractor must review and maintain the ATO in accordance with HHS*/*HRSA policies*.*
         * E‐Authentication (E‐Auth) Risk Assessment Questionnaire
         * Privacy Threshold Analysis (PTA)
         * Privacy Impact Assessment (PIA)
         * Risk Assessment Report
         * IT System Business Impact Analysis (BIA)
         * IT System Contingency Plan (CP)
         * IT System CP Test Results
         * System of Record Notice (SORN)
         * Interconnection Agreements/Service Level Agreements/Memorandum of Agreements
         * Configuration Management Plan
         * Security Configurations
         * FedRAMP Test Procedures and Results
         * Security Assessment Plan (SAP)
         * Security Assessment Report (SAR)
         * System Security Plan (SSP)
         * Plan of Action and Milestones (POA&M)
         * Continuous Monitoring Plan
         * Incident Response Plan
         * FedRAMP Control Tailoring Workbook
         * Control Implementation Summary Table
         * Results of Penetration Testing
         * Software Code Review
   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 FedRAMP Security Control Baseline/Continuous Monitoring controls and the contractor's implementation status as documented in the Security Assessment Report and related Continuous Monitoring artifacts. In addition, the contractor 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.
      1. All vulnerabilities and findings must be remediated, in accordance with timelines based on their residual risk as specified in the HHS POA&M Standard and HHS Policy for Vulnerability Management: (1) critical vulnerabilities no later than ***fifteen (15) days*** from discovery date and (2) high within **thirty (30) days** from discovery date and (3) medium within **ninety (90) days** from discovery date and (4) low vulnerabilities no later ***than three hundred and sixty five (365) days*** from discovery date***.***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. The HRSA VM team and the ISSO will determine the risk rating of vulnerabilities. The HRSA CISO may direct out of band patching due to potential active exploit, zero day vulnerability, etc.
   5. **Revocation of a Cloud Service**. HHS*/*HRSA have the right to take action in response to the CSP's lack of compliance and/or increased level of risk. In the event the CSP fails to meet HHS and FedRAMP security and privacy requirements and/or there is an incident involving sensitive information, HHS and/or HRSA 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.
4. 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. *[HRSA include meetings/deliverables timelines as applicable/necessary]*
   2. At a minimum, the Contractor must provide the following artifacts/deliverables on a monthly basis:
      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 HRSA 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/HRSA'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.
5. 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*/*HRSA 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.
6. Incident Reporting
   1. The Contractor (and/or any subcontractor) must provide an Incident and Breach Response Plan (IRP) in accordance with HHS, HRSA, OMB, and US-CERT requirements and obtain approval from the OpDiv. In addition, the Contractor must follow the incident response and US-CERT reporting guidance contained in the FedRAMP 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*/*HRSA personnel, or agents acting on behalf of HHS/HRSA*,*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.
7. 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.
8. 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 are in compliance with 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 certificate from the NIST CMVP that provides for origin authentication, data integrity, and signer non-repudiation.

**V.  Other IT Procurements**

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.

**Frequently, the technology to be deployed and data to be collected to meet the statement of work change throughout the period of performance. The following Optional tasks may be exercised during the Base and Option Periods of the contract.**

**Other IT Procurements (INFORMATION SECURITY OPTIONAL TASK #1)**

1.  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)) 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.  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.

3.  Physical Access to Government Controlled Facilities

"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."

### Task Area 12: Capital Planning and Investment Control and Earned Value Management

Capital Planning and Investment Control (CPIC) is an integral part of the Agency's strategic planning initiative. In accordance with the CPIC process, Clinger-Cohen Act, and Federal Information Technology Acquisition Reform Act (FITARA), the Contractor shall follow the HHS/HRSA CPIC framework and provide complete, reliable, consistent, and timely life-cycle information, to include development and cost information for qualifying projects; and systematic measurement of performance. Within 90 days of task award, the Contractor must conduct an Integrated Baseline Review (IBR) in accordance with the DHHS and HRSA requirements, if applicable. Additionally, the Contractor shall prepare and submit a monthly project management report in the government-desired format, as specified by the HRSA CPIC guidance.

1. ​Capital Planning and Investment Control (CPIC).

Capital Planning and Investment Control (CPIC). Submit progress reporting to the COR and OPTN PIMS representatives for the HRSA CPIC process, including detailed monthly invoicing with labor costs (i.e., hours/staff (rates)/task), other direct and indirect costs, and fees by the 5th business day of the month following the reporting period. The report data should include all relevant data needed to populate the HRSA CPIC reporting tool (Folio).

1. ​Earned Value Management (EVM)

Track cost, schedule and scope through EVM reports for all development projects. This information shall be included in the Monthly CPIC Report.

* 1. Apply and manage tasks in accordance with HRSA’s EVM policy. The Contractor shall incorporate an EVM System throughout the full life-cycle.
  2. Use Microsoft Project 2010 or equivalent HRSA-approved software to provide project status information at WBS level 3, with capability to report at any lower level at the request of the COR.
  3. The EVM Monthly reports shall contain the following information:
     + Budgeted (planned) Cost for Work scheduled (BCWS) = Planned Value
     + Budgeted Cost for Work Performed (BCWP) = Earned Value
     + Actual Cost of Work Performed (ACWP) = Actual Cost
     + Budget at Completion (BAC)
     + Estimate at Completion (EAC), and
     + Performance curve graph plotting cumulative BCWS, BCWP, and ACWP on a monthly basis from inception of the agreement, with BCWS plotted to completion and projecting the ACWP curve to the Estimate at Completion (EAC) value. (Data will be extracted from MS Project and plotted in MS Excel.)
     + EVMs variance analysis:
       - Cost Variance = (BCWP - ACWP);
       - Cost Variance % = (CV / BCWP x 100%);
       - Cost Performance Index (CPI) = (BCWP / ACWP);
       - Schedule Variance = (BCWP – BCWS
       - Schedule Variance % = (SV / BCWS x 100%);
       - Schedule Performance Index (SPI) = (BCWP / BCWS);
       - Explain the reasons for all variances that exceed the statutory threshold of +10 percent or a lower threshold specified in the contract;
       - Define technical performance variance. Explain, based on work accomplished as of the date of the report, whether the performance goals will be achieved, and the impact to the cost and schedule goals.

Deliverable: Contractor will provide required deliverable for contract threshold in accordance to the HRSA CPIC Policy by the 5th business day of each month.

### Task Area 13: Enterprise Project Life Cycle (EPLC)

All OPTN PIMS EHBs development and enhancement activities shall follow the HRSA Enterprise Project Life Cycle (EPLC). This task order covers activities across the EPLC such as usability studies, requirements analysis, design, development, and implementation. EPLC aligns closely with waterfall software development methodology, which may be used for major new development efforts.

However, streamlined or "tailored" EPLC processes with reduced documentation and gate review requirements may be used for short-cycle agile projects.

The contractor shall prepare comprehensive documentation supporting all activities. This includes preparing a design and implementation document, maintaining data models, maintaining business rules documents, preparing testing plans and recording results, as well as all code developed for the system. Task Area 13: EPLC under the deliverables section on page 43 describes potential artifacts for all the phases. The Project Process Agreement (PPA) will be provided to tailor the EPLC requirements in terms of justifications for selection, substitution or omission of specific reviews, deliverables, and other EPLC components relevant to this project.

Deliverable: Contractor will provide required deliverable for contract 5 Business days before the scheduled gate review.

### Task Area 14: Personnel Security Requirements

**Background Investigation Requirements**

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).

**Position Sensitivity Designations**

The following position sensitivity designation levels apply to this solicitation/contract:

* **non sensitive, moderate risk public trust Tier 2 investigation**
* **non sensitive, high risk public trust Tier 4 investigation (this level applies when elevated rights are needed for system access.)**

**RESIDENCY REQUIREMENTS FOR FOREIGN NATIONALS**

Under the requirements for fitness for duty as described in EO 13467 and in conjunction with Homeland Security Presidential Directive-12 (HSPD-12), OPM can complete a background investigation only for persons who have resided in the U.S. for a total of **at least three (3) of the past five (5)** **years**. The residency requirements apply only to foreign nationals. If any prospective foreign national contractor/subcontractor employee does not meet the residency requirements, Please do not send their name forward as a potential team member.

**BACKGROUND INVESTIGATIONS**

The Contractor shall advise its prospective employees about the background investigation requirements stated herein.

If a Contractor employee changes job responsibilities under this contract, the Contractor shall notify the COR, and the Government will make a determination whether an upgraded investigation is required.

In the event there are any proposed personnel changes in the Contractor’s staffing roster previously submitted to the COR, the Contractor shall submit an updated roster to the COR, along with a brief explanation for the change. In turn, the COR will initiate the procedures stated herein to ensure any new contractor employees completes the investigation process up to and including if needed, obtain a PIV card in a timely manner – **prior to that individual commencing work under the contract.**

For any individual who is cleared to start work but upon completion of the investigative process does not obtain a favorable background investigation he/she shall cease work on the contract immediately.

With the exception of costs associated with fingerprinting Contractor employees outside of the HRSA Personnel Security Office, the Government will conduct all required background investigations at no cost to the Contractor. The cost of fingerprinting Contractor employees at any location other than the HRSA Personnel Security Office will be borne by the Contractor. Every effort will be made to schedule contractors at a location that will not charge a fee for the fingerprints.  Contractors who hold or have previously held a Government security clearance shall advise the HRSA Personnel Security Staff of the details of such clearance.

During a fingerprint appointment, each contractor employee must present two (2) forms of identification as part of the identity proofing process.  One form of identification must be a State or federal government-issued photo identification document. Acceptable forms of identification are listed below.

List of acceptable documents for Identity Proofing **one of which must be**:

* Drivers License or ID card that is compliant with REAL-ID requirement
* US Passport or Passport Card
* Permanent Resident Card or Alien Registration Receipt Card  (Form I-551)
* Employment Authorization Document that contains a photograph (Form I-766)
* US Military ID Card
* US Military dependents ID card
* PIV Card

Second form of ID can be one of the following:

* ID card issued by a federal, state, or local government agency or entity, provided that it contains a photograph
* voter’s registration card
* U.S. Coast Guard Merchant Mariner Card
* Certificate of U.S. Citizenship (Form N-560 or N-561)
* Certificate of Naturalization (Form N-550 or N-570)
* U.S. Citizen ID Card (Form I-197)
* Identification Card for Use of Resident Citizen in the United States (Form I-179)
* Certification of Birth Abroad or Certification of Report of Birth issued by the Department of State (Form FS-545 or Form DS-1350)
* Reentry Permit (Form I-327)
* Employment authorization document issued by the Department of Homeland Security (DHS)
* driver’s license issued by a Canadian government entity
* Native American tribal document
* U.S. Social Security Card issued by the Social Security Administration
* original or certified copy of a birth certificate issued by a state, county, municipal authority, possession, or outlying possession of the United States bearing an official seal (if name is now different you must also provide the legal document that changed the name)

An individual who receives an unfavorable report may appeal that finding by submitting a written request to the DSS at [ps-updates@hrsa.gov](mailto:ps-updates@hrsa.gov)

Background investigations will be conducted by the Defense, Counter Intelligence and Security Administration (DCSA)

**PERSONAL IDENTITY VERIFICATION (PIV) CARDS**

All Contractor employees (including subcontractors) must possess a PIV card that was issued based on a current background investigation that resulted in   a favorable determination where one of the following applies:

* Will be working in HHS-owned or leased space (PIV card required)
* will have access to HHS equipment or systems (PIV card required)

All PIV cards shall remain the property of the Federal Government. At any time, if a Contractor employee is terminated or otherwise ceases work under the contract, or no longer requires a PIV Card for contract performance purposes, the Contractor shall collect the individual’s PIV card and immediately notify HRSA Personnel Security Staff in writing by submitting an email to [ps-updates@hrsa.gov](mailto:ps-updates@hrsa.gov) , with copies to the respective COR and Contracting Officer. The Contractor shall immediately return the PIV Card(s) to the COR who will immediately return them to the Division of Security Services.

Like PIV Cards, other Government-issued Access Cards are Government property, Contractors and Contractor Employees are hereby placed on notice that any abuse, destruction, defacement, unauthorized transfer or withholding (i.e., failure to return to the Government) may be punishable to the greatest extent of the law.

Unauthorized possession of a PIV Card, or any other type of Government-issued Access Card, and/or willfully allowing any other person to have or to use your Access Card, is prohibited and can be criminally prosecuted under 18 U.S.C. §§ 499 and 70I, which prohibit photographing or otherwise reproducing or possessing HHS identification cards in an unauthorized manner, under penalty of fine, imprisonment, or both. Wrongdoers may also be held financially responsible for any/all civil and equitable remedies – to include, but not limited to, damages for any pecuniary loss suffered by the Government as a result of any of the above-listed actions or failure to act.

# Deliverables

The contractor shall ensure all products and services delivered under this contract are compliant with Section 508 in accordance with the Health and Human Services Acquisition Regulation (HHSAR). These Section 508 Standards were issued by the [**United States Access Board**](https://www.access-board.gov/)(https://www.access- board.gov/) and published in the Federal Register, on January 18, 2017, as the **final rule** (https[://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-](http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-) refresh/final-rule). The final rule updates the Section 508 Standards along with accessibility guidelines for telecommunication products and equipment covered by section 255 of the Communications Act.

The Section 508 Standards applicable to this contract are:

**Section 508 Standards and Guidelines** (https[://www.access-board.gov/guidelines-and-](http://www.access-board.gov/guidelines-and-) standards/communications-and-it/about-the-ict-refresh/final-rule/text-of-the-standards-and-guidelines)

* Web Content Accessibility Guidelines (WCAG) 2.0
  + Success Criteria, Level A and AA
* Chapter 3: Functional Performance Criteria (FPC)
* Chapter 4: Hardware (If Applicable)
* Chapter 5: Software
* Chapter 6: Support Documentation and Services

Section 508 requires that all external public facing content and non-public facing official agency communications be accessible. Regardless of format, all digital content or communications materials produced as deliverables under this contract must conform to applicable Section 508 standards to allow federal employees and members of the public with disabilities to access information that is comparable to information provided to persons without disabilities.

The contractor shall complete and submit the applicable **HHS Section 508 Accessibility Compliance Checklist** per Section 508 deliverable. The checklist will serve as an artifact declaration of the Section 508 deliverable's compliance. Remediation of any Section 508 deliverables that do not comply with the applicable requirements as set forth below shall be the contractor's responsibility.

HHS guidance and checklists regarding accessibility of documents can be found at https://[www.hhs.gov/web/section-508/accessibility-checklists/index.html.](http://www.hhs.gov/web/section-508/accessibility-checklists/index.html)

The **HHS Section 508 Product Assessment Template (PAT)** that is referenced above in 352.239-78 Electronic Information and Technology Accessibility Notice, Paragraph (c), ***has been replaced*** with the **Voluntary Product Accessibility Template Version (VPAT) 2.1 or later,** and is considered to meet HHS PAT requirement. The new form can be downloaded from **https:**[**//www.itic.org/policy/accessibility/vpat**.](http://www.itic.org/policy/accessibility/vpat)

**NOTE: ICT vs. EIT**

Procurement documentation from HHS or other agencies may contain references to "EIT" (Electronic and Information Technology) and "ICT" (Information and Communications Technology). HHS considers these terms to be interchangeable, and "EIT" should always be interpreted to be "ICT" in any HHS procurement.

Deliverables: HHSAR Clause 352.239-78 and 352.239-79 are applicable.

Most deliverables will be determined at the order level. All deliverables, including data deliverables, shall be useable by the Government, including submission in useable formats and with adequate accompanying documentation to enable their use. The deliverables listed below are common minimum requirements for IT procurements.

Task Area 10: Records Management Requirements

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Task** | **Description** | **Quantity** | **Format** | **Delivery Date** |
| 10 | Provide Records Management training completion certificates | As needed | PDF | Within 30 days after contract award and upon new staff onboarding and thereafter completing the annual refresher course during the life of the contract |

Task Area 11: HHS Policy for Information Technology Procurements - Security and Privacy Language

| **Policy Section** | **Deliverable Title/Description** | **Due Date** |
| --- | --- | --- |
| **Roster** | Roster | Within 14 days of the effective date of this contract. |
| **Contractor Employee Non-Disclosure Agreement (NDA)** | Contractor Employee Non-Disclosure Agreement (NDA) | Prior to performing any work on behalf of HHS |
| **Privacy Threshold Analysis (PTA)/ Privacy Impact Assessment (PIA)** | Assist in the completion of a PTA/PIA form | Within 60 days after contract award |
| **Training Records** | Copy of training records for all mandatory training | In conjunction with contract award and annually thereafter or upon request |
| **Rules of Behavior** | Signed ROB for all employees | Initiation of contract and at least annually thereafter |
| **Incident Response** | Incident Report (as incidents or breaches occur) | As soon as possible and without reasonable delay and no later than 1 hour of discovery |
| **Incident Response** | Incident and Breach Response Plan | Upon request from government |
| **Personnel Security Responsibilities** | List of Personnel with defined roles and responsibilities | Before an employee begins working on this contract. |
| **Personnel Security Responsibilities** | Off-boarding documentation, equipment and badge when leaving contract | Within 14 days after the Government's final acceptance of the work under this contract, or in the event of a termination of the contract. |
| **Background Investigation** | Onboarding documentation when beginning contract. | Prior to performing any work on behalf of HHS |
| **Certification of Sanitization of Government and Government Activity-Related Files, Information, and Devices.**[**[28]**](https://intranet.hhs.gov/policy/hhs-policy-information-technology-procurements-security-and-privacy-language#ftn28) | Form or deliverables required by OpDiv. | Within 14 days of the employee's exit from the contract |
| **Contract Initiation and Expiration** | If the procurement involves a system or cloud service, additional documentation will be required, such as Disposition/Decommission Plan | Within 14 days of the employee's exit from the contract |
| **Assessment and Authorization (A&A)** | A&A Package   * SSP * SAR * POA&M * Authorization Letter * CP and CPT Report * E-Auth (if applicable) * PTA/PIA (if applicable) * Interconnection/Data Use Agreements (if applicable) * Authorization Letter * Configuration Management Plan (if applicable) * Configuration Baseline * Other OpDiv-specific documents | 30 days prior to the Operational Readiness Review (ORR) to the Contracting Officer (CO) and/or Contracting Officers Representative (COR) |
| **Protection of Information in a Cloud Environment** | Contract expiration | 30 days prior to the Operational Readiness Review (ORR) to the Contracting Officer (CO) and/or Contracting Officers Representative (COR) |
| **A&A Process for Cloud Services** | A&A Package   * SSP * SAR * POA&M * CMP * CP and CPT Report * E-Auth (if applicable) * PTA/PIA (if applicable) * Penetration Test Results * Interconnection/Data Use/Agreements (if applicable) * Service Level Agreement * Authorization Letter * Configuration Management Plan (if applicable) * Configuration Baseline * Other OpDiv-specific documents | 30 days prior to the Operational Readiness Review (ORR) to the Contracting Officer (CO) and/or Contracting Officers Representative (COR) |
| **Reporting and Continuous Monitoring** | * POA&M updates * Revised security documentation/Agreements | Monthly/as requested by HRSA |
| **Incident Reporting** | * Incident reports (as needed) * Incident Response Plan | Incident Reports – must respond to all alerts/Indicators of Compromise (IOCs) provided by HHS Computer Security Incident Response Center (CSIRC)/HRSA Computer Security Incident Response Team ([hrsacsirt@hrsa.gov](mailto:hrsacsirt@hrsa.gov)) within **24 hours**  Report all suspected and confirmed information security and privacy incidents and breaches to the HRSA Computer Security Incident Response Team as soon as possible and without unreasonable delay, no later than **one (1) hour**  Incident Response Plan - 30 days prior to the Operational Readiness Review (ORR) to the Contracting Officer (CO) and/or Contracting Officers Representative (COR) |
| **Other IT Procurements (Non-Commercial and Open Source Computer Software Procurements)** | * Computer software, including the source code. | Prior to performing any work on behalf of HHS |

Task Area 13: Enterprise Project Life Cycle (EPLC)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Deliverable** | | **Ownership** | **Approach** | **Date** |
| **Planning Phase** | | | |
| Project Management Plan (PMP) | | Program Project Lead, Contractor | The Program project lead and the contractor will prepare the PMP after discussions with COR and appropriate stakeholders. The plan will also address the scope, budget and schedule. | Within 45 days after task is exercised |
| Project Work Breakdown Structure (WBS)/Schedule | | Contractor | The Program Project Lead will develop a contract/project level WBS using Microsoft project software. | Within 45 days after task is exercised |
| Release WBS/Schedule | | Contractor | The Program Project Lead will develop a schedule and detailed list of tasks for each of the major releases. | Based upon WBS |
| Project Budget | | Program Project Lead, Contractor | The contractor will develop a detailed budget prior to the commitment of resources for any development activities. | Within 45 days after task is exercised |
| Schedule Activity List | | Contractor | The Program Project Lead will develop a detailed list of activities in consultation with the stakeholders. | Once a month |
| Resource Requirements Log | | Contractor | The Program Project Lead will develop a detailed software and hardware resource requirements as part of the infrastructure plan. | Based upon project plan |
| Risk Management Log | | Program Project Lead, Contractor | The Program Project Lead will log all the major project risks in the risk log/register and communicate it to the stakeholders | Monthly (as well as when new risks are identified) |
| Training Plan | | Program Project Lead, Contractor | A training plan will be developed which would provide details, including the training approach, training courses offered, duration of each course, intended audience(s). | Based upon project plan |
| **Requirements Phase** | | | | |
| Business Process Definition (BPD) | | Contractor | Based upon discussions with the business owners, this document will capture the appropriate business processes. This information will be used to drive additional requirements elaboration activities such as the creation of screen mockups. | Based upon project plan |
| Business System Requirements (BSR) Document | | Contractor | A requirements document reflecting the high level capabilities and attributes of the desired solution will be created. | Based upon project plan |
| Release-  Level Requirements  /RTM | | Contractor | This document will provide of the traceability of project level and release level requirements to the functionality contained within a specific release. | Based upon project plan |
| Logical Data Model | | Contractor | The logical data model provides a way to represent the business processes (and depicts the relationship between them). This document will be used to further elaborate the system requirements. | Based upon project plan |
| **Design Phase** | | | | |
| Technical Design Document (TDD) | | Contractor | This document will explain the system design and architecture. | Based upon project plan |
| Physical Data Model | | Contractor | The Physical Data Model will take the logical data model information and create the physical data model structures. This will be developed in compliance with all appropriate EHBs naming conventions and standards. | Based upon project plan |
| Data Dictionary | | Contractor | This document would explain the detailed definitions for all tables and columns. | Based upon project plan |
| **Test Phase** | | | | |
| Test Plan | | Contractor | The test plan would define the overall plan for performing the QA testing activities for the project. It would contain the proposed testing approach, types of testing that will performed, and details about the testing tools that will be used.. | Based upon project plan |
| Test Scripts/Cases | | Contractor | Describes the detailed test scripts and test cases that will be used to validate that the system functions as expected. The contractor will work with the business owners to ensure that the test cases developed exercise all of the business areas/functions of the system. | Based upon project plan |
| Testing Defects Resolution Report | | Contractor | An export of the issues from the issue tracker will be provided so the stakeholders can get the insight into the issues found during contractor's internal testing and their latest status. | Based upon project plan |
| Implementation/ Deployment Plan | | Contractor | The implementation plan will provide details about how the system will be installed and made operational in the production environment for each of the major releases. | Based upon project plan |
| **Operations & Maintenance Phase** | | | | |
| Operational Readiness Review | | Program Project Lead, Contractor | The Review will ensure that configuration and testing have been completed, documentation has been written and approved, deployment packages have been written and tested, security testing completed, and all other EPLC requirements have been met. | Based upon project plan |
| Lessons Learned | | Program Project Lead, Contractor | A lessons learned document will be created to understand what worked well (and what didn't) in the last release so that this experience can be used to improve the techniques used to develop future releases/systems. | 45 days after production implementation |
| Patch Release/Deployment Plan | | Contractor | This plan will provide the details about potential impacts/dependencies, and how to apply the patch in the production environment. | Based upon project plan |

# Appendices

Appendix A – Contractor Non-Disclosure Agreement

Appendix A – Contractor Non-Disclosure Agreement

**Contractor Non-Disclosure Agreement**

**Information Technology Systems Security Contractor Non-Disclosure Agreement**

Access to sensitive information (such as personally identifiable information [PII]), non-public information, confidential information, and/or Controlled Unclassified Information (CUI) from the files of the Department of Health and Human Services (HHS) is required in the performance of my official duties, under contract number between (HHS/HRSA and my employer (Employer’s Name) .

I agree that I shall not release, publish, or disclose such information to unauthorized personnel, and I shall protect such information in accordance with relevant laws and regulations.

I affirm that I have received a written and/or verbal briefing by my company concerning my responsibilities under this agreement. I understand that violation of this agreement may subject me to criminal and civil penalties.

Signed:

Type or Print Name:

Date:

Witnessed by:

Date:

Copies are to be retained by: HRSA Contracting Officer Representative

Contractor’s Contract Management

Individual Signatory