U.S. DEPARTMENT OF DEFENSE
DEFENSE HEALTH AGENCY
PERFORMANCE WORK STATEMENT

eCTD SOFTWARE LICENSE, MAINTENANCE, TECHNICAL SUPPORT SERVICES, AND TRAINING FOR eCTD PUBLISHING AND REVIEWING SOFTWARE PRODUCTS AND MODULES

ENTERPRISE INFORMATION TECHNOLOGY (eIT)
PROJECT MANAGEMENT OFFICE (eIT PMO)

Solicitation Number: HT942726RE0050001
Version: 2
Date: 22 June 2026

PART 1

1. GENERAL INFORMATION

1.1 This is a non-personal services contract to provide Electronic Common Technical Document (eCTD) software license and templates, maintenance, technical support services, and training for eCTD publishing and reviewing software products and modules.

1.2 Description of services/introduction:

The Contractor shall provide commercial off-the-shelf (COTS) eCTD publishing and reviewing software licenses, non-personal services necessary to perform eCTD software license, maintenance, technical support services, and training for eCTD publishing and reviewing software products and modules as defined in this Performance Work Statement (PWS) except for those items specified as Government furnished property and services. The Contractor shall perform to the standards described in this PWS.

1.3 Background:

The eCTD Publisher System is intended for use by eIT PMO customers/user base for preparation and lifecycle maintenance of electronic regulatory submissions originating from the Army Office of the Surgeon General (OTSG) sponsored investigational product development. The critical function of the system is the ability to generate electronic regulatory submissions. In addition, the system shall have the ability to automate workflow steps required to manage preparation of electronic submissions for submission to regulatory agencies (e.g., the U.S. Food and Drug Administration [FDA]).

1.4 Objectives:

The eCTD publishing system shall be used for:

- Preparation and lifecycle maintenance of electronic regulatory submissions
- Greater efficiency within regulatory submissions by reducing manual publishing steps, minimizing rework, and decreasing submission preparation timelines
- A higher level of compliance with applicable regulations through system validation, standardized templates, and automated validation checks

The eCTD publishing system shall have the ability to:

- Scale to support increases in the number of electronic regulatory submissions resulting from expanding clinical trial activities, including multiple concurrent preparation and review activities, without degradation of system performance
- Provide seamless access to third parties (e.g., external regulatory reviewers, CROs, etc.)
- Integrate the eCTD publishing system with other key Defense Health Agency (DHA) systems (e.g., Open Text – Content Server)

1.5 Scope:

The eIT PMO needs to acquire software licenses and maintenance for twelve (12) eCTD Publisher user accounts and up to fifty (50) named eCTD reviewer accounts. Additional services required are FDA-mandated submission templates, technical support services for resolving application problems, training services for both the eCTD publishing and reviewing users, FDA-validated software installation support and scripts, and non-personal services to support regulatory questions by eCTD publishers.

1.6 Period of Performance:

The anticipated period of performance of this contract is 15 July 2026 through 14 January 2032. There will also be four (4) one-year renewable options and a six (6) month extension to be

exercised at the discretion of the Government (total potential of a five-and-one-half-year (5.5 year) contract).

- Base Period: 15 July 2026 – 14 July 2027
- Option Period 1: 15 July 2027 – 14 July 2028
- Option Period 2: 15 July 2028 – 14 July 2029
- Option Period 3: 15 July 2029 – 14 July 2030
- Option Period 4: 15 July 2030 – 14 July 2031
- 6-month extension: 15 July 2031 – 14 Jan 2032

The Contract Specialist will notify the Contractor of the intent to exercise an option year 90 calendar days before the option is to be exercised.

1.7 Administrative specifications:

Place of performance: The work shall be performed remotely.

1.7.1 Recognized Federal holidays:

Contractor is not required to perform on the following holidays:
New Year's Day
Labor Day
Martin Luther King Jr.'s Birthday
Columbus Day
President's Day
Veteran's Day
Memorial Day
Thanksgiving Day
Juneteenth Day
Christmas Day
Independence Day

1.7.2 Hours of operation:
The Contractor is responsible for conducting business Monday through Friday, except for federal holidays. The Contractor must at all times maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS.

1.7.3 Emergency Services:
On occasion, services may be required to support an activation or exercise of contingency plans outside the normal duty hours.

1.8 Contractor travel:
(Reimbursable) Travel cost estimate for in-person trainings or for technical consulting support held at Fort Detrick to fully support end users and administrators. See PWS Sections 5.3 (Task 3: Training Consulting and Technical Support Services) 5.4 (Task 4: Travel).

1.9 Other Direct Costs (ODC): The Government intends to utilize "Plugged" Not-to-Exceed (NTE) amount for all ODCs listed.

1.10 Quality

1.10.1 Quality Control (QC):
The Contractor shall develop and maintain an effective QC program to ensure services are performed in accordance with this PWS. The Contractor shall develop and implement procedures to identify, prevent, and ensure nonrecurrence of defective services. The Contractor's QC program is how the work complies with stated requirements. A Quality Control Plan (QCP) (**Deliverable 1**) will initially be submitted NLT thirty (30) calendar days after contract award (DACA). After acceptance of the QCP, the Contractor shall receive the CO's acceptance in writing of any proposed change to the QC system.

1.10.2 Quality assurance (QA):
The Government will evaluate the Contractor's performance under this contract in accordance with the Quality Assurance Surveillance Plan (QASP). This plan provides a systematic method for the Government to evaluate performance and to ensure that the Contractor has performed in accordance with the performance standards. It defines how the performance standards will be applied, the frequency of surveillance, and the minimum acceptable defect rate(s).

1.11 Contractor Personnel

1.11.1 Data rights:
The Government will have unlimited data rights to all products modified or support provided to COTS systems.

1.12 Reporting

1.12.1 Service Contract Reporting (SCR):
Service contractor reporting of information is required in the System for Award Management (SAM) for:

- Contract Awards, no IDVs
- Contract Awards include purchase orders, delivery/task orders, BPA calls, and definitive contracts
- Service Contracts, i.e., any PSC that starts with a letter excluding utility PSCs (S110, S111, S112, S114, and S119)
- All cost-reimbursement, time-and-materials, and labor-hour service contracts with an estimated total value > $150,000 and base date signed is between 10/1/13 and 9/30/18.
- Fixed Price Contracts: If the contract's base date signed AND base effective date is between 10/01/2013-09/30/2014, the total contract value must be >= $2.5M

- Fixed Price Contracts: If the contract's base date signed AND base effective date is between 10/01/2014-09/30/2015, the total contract value must be >= $1M
- Fixed Price Contracts: If the contract's base date signed AND base effective date is between 10/01/2015-09/30/2018, the total contract value must be >= $500,000

Steps for Submitting a Service Contract Report (SCR)
1. Go to www.sam.gov and log in.
2. Select Entity Registrations and then select Service Contract Reporting.
3. SAM displays your entities which have service contracts and meet the reporting criteria. Select View by entity to see the service contracts for each entity.
4. Next, select Add for the service contract against which you want to create a Service Contract Report. Each service contract which meets the FAR Subpart 4.1703 reporting thresholds is displayed.
5. You will be taken to the Complete Service Contract Report page. SAM displays the contract details and allows you to report. You are required to enter the following information:

- Total Amount Invoiced: Total dollar amount invoiced for services performed during the previous Government fiscal year under the contract (this amount should include the prime and any subcontract amount).
- Prime Contractor Hours Expended: Prime contractor direct labor hours expended on the services performed during the previous Government fiscal year. The amount you enter is automatically divided by 2,080 hours to calculate a Full Time Employee (FTE) equivalent, displayed under the Prime Contractor Hours Expended as Prime Contractor FTEs.

6. Report any required Tier 1 subcontractor information by selecting the Add Tier 1 Subcontract Information button.
7. When you are ready to submit the report, select Submit. This saves your report and returns you to the Select Service Contract page where you can create other SCRs or edit an existing SCR.

1.12.2 Non-Disclosure Agreement (NDA):
All Contractor personnel who obtain and/or will obtain access to proprietary, classified, or confidential information or any information release of which is protected or governed by law or regulation associated with DHA acquisitions shall be required to complete and sign a DHA Contractor NDA (DHA Form 49) (**Deliverable 2**) prior to beginning work on the subject contract. The Contractor shall execute an NDA on behalf of the company and shall ensure that all assigned staff (including all other personnel performing on contract/task order) execute an NDA protecting the procurement sensitive information of the Government and the proprietary information of other Contractors. The NDA shall be executed no later than the first day of employment and is to be renewed upon exercising a contract option period. Assignment of staff who have not executed this statement or failure to adhere to this statement shall constitute default on the part of the Contractor. The Contractor shall maintain originally-signed NDAs of individual employees and provide copy to the COR.

1.12.3 Government's COR:
The COR monitors all technical aspects of the contract and assists in contract administration. The COR is authorized to perform the following functions: assure that the Contractor performs the technical requirements of the contract; perform inspections necessary in connection with contract performance; maintain written and oral communications with the Contractor concerning

technical aspects of the contract; issue written interpretations of technical requirements, including Government drawings, designs, specifications; monitor Contractor's performance and notify both the CO and Contractor of any deficiencies; coordinate availability of Government furnished property; and provide site entry of Contractor personnel. A letter of designation issued to the COR, a copy of which is sent to the Contractor, states the responsibilities and limitations of the COR, especially regarding changes in cost or price, estimates or changes in delivery dates. The COR is not authorized to change any of the terms and conditions of the resulting contract.

- Provide the COR and contract specialist with a monthly status report (**Deliverable 3**) via email submitted by the 5th calendar day of each month. This report shall address each element of the QASP for ease of COR evaluation and will include status of all work in progress, as well as track work which has been requested by eIT PMO, but which has not yet been performed. The monthly report shall include cost estimates for any such work.
- Provide the COR a monthly project burn report (**Deliverable 4**) including funds remaining on each CLIN, estimates for outstanding invoices (for work that has been performed but not yet invoiced), and estimates for outstanding invoices. Provide this report via email submitted by the 5th calendar day of each month.
- Provide ad-hoc reporting completely and accurately if additional information is requested or more explanation is needed.
- Perform data analyses and ad hoc reporting to support the eIT PMO management activities such as briefing materials, reports, taskers, memos, procedures, etc.
- All vendor-supplied documents must be converted to eIT PMO approved template/format prior to delivery/demonstration to the customer.

1.12.4 Post award conference/periodic progress meetings:

The Contractor agrees to attend any post-award conference convened by the contracting activity or contract administration office in accordance with FAR Subpart 42.5. The CO, COR, and other Government personnel, as appropriate, may meet periodically with the Contractor to review the Contractor's performance. At these meetings the CO will apprise the Contractor of how the Government views the Contractor's performance and the Contractor will apprise the Government of problems, if any, being experienced. Appropriate action shall be taken to resolve outstanding issues. These meetings shall be at no additional cost to the Government.

1.13 Contractor Identification

1.13.1 Contractor personnel performing services in a Contractor capacity in a Government facility are required to possess and wear an identification badge that displays his or her name and the name of their company. All Contractor personnel shall identify themselves as Contractor support personnel in all forms of communication with all entities with whom DHA/Deputy Assistant Director for Acquisition & Sustainment (DAD A&S)/Head of the Contracting Activity (DHACA) has business dealings. The Contractor shall:

- Answer all telephone calls and have a personalized voice message with an introductory statement that includes the fact that the person is Contractor support personnel
- Ensure all those with whom the person interacts in any face-to-face dealings while supporting the DAD A&S understands that the person is Contractor support personnel
- Include a title block in all emails that states the fact that the person is Contractor support personnel
- Ensure all those with whom the person interacts in any face-to-face dealings while supporting DHA/DAD A&S/DHACA understands that the person is Contractor support personnel

1.13.2 Contractor personnel will be required to attend meetings or otherwise communicate with Government and/or other contract representatives to meet the requirements of this order.
1.13.3 Contractor personnel, while performing in a Contractor capacity, are prohibited from using their retired or reserve component military rank or title in any written or verbal communications associated with the contracts in which they provide services.

1.14 Contractor Access to Health Affairs (HA)/DHA Network(s): RESERVED

1.15 Personal Security

1.15.1 The Contractor shall comply with DoD 8570.01-M, "Information Assurance Workforce Improvement Program, CH4" November 10, 2015 as amended; 8500.01, "Cybersecurity", dated March 14, 2014; DoD Manual (DoDM) 6025.18, "Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule Compliance in DoD Health Care Programs", dated March 3, 2019, Department of Defense Instruction (DoDI) 6025.18 "HIPAA Privacy Rule Compliance in DoD Health Care Programs", dated March 13, 2019; and DoDM 5200.02 "Procedures for the DoD Personnel Security Program (PSP)," incorporation change three (3), effective September 24, 2020. Contractor responsibilities for ensuring personnel security include, but are not limited to, meeting the following requirements:

1.15.1.1 Follow the DHA Personnel Security Office guidelines for submittal of security clearances. Contact the DHA Personnel Security Office for guidance on the appropriate background investigation required for personnel on the contract. The DHA Personnel Security Office can be reached at (703) 275-6038.

1.15.1.2 Initiate, maintain, and document personnel security investigations appropriate to the individual's responsibilities and required access to Controlled Unclassified Information (CUI).

1.15.1.3 DHA Personnel Security Office does not deny any access to any automated information system (AIS), network, or Controlled Unclassified Information (CUI). If a Contractor receives an unfavorable background investigation, the request for access will be sent back to the FSO for further action. Any unfavorable adjudication will result in DHA Personnel Security Office not signing-off on any access request.

PART 2

2. DEFINITIONS, ACRONYMS, AND APPLICABLE PUBLICATIONS/ INSTRUCTIONS

2.1 Definitions:

2.1.1 Category D: Information Technology (IT) and Telecommunications Services (called D-Services)

2.1.2 Category R: Support (Professional/Administrative/Management) Services (called R-Services)

2.1.3 Contracting Officer (CO): A person with the authority to enter into, administer, and/or terminate contracts and make related determinations and findings.

2.1.4 Contracting Officer's Representative (COR): An individual, including a contracting officer's technical representative (COTR), designated and authorized in writing by the CO to perform specific technical or administrative functions. This individual does NOT have authority to change the terms and conditions of the contract.

2.1.5 Nonpersonal services contract: A contract under which the personnel rendering the services are not subject, either by the contract's terms or by the manner of its administration, to the supervision and control usually prevailing in relationships between the Government and its employees.

2.1.6 Quality Assurance Surveillance Plan (QASP): An organized written document specifying the surveillance methodology to be used for surveillance of Contractor performance. The Government may either prepare the QASP or require the offerors to submit a proposed quality assurance surveillance plan for the Government's consideration in development of the Government's plan.

2.2 Acronyms:

AIS	Automated Information System
APL	Approved Products List APL
AQL	Acceptable Quality Level
ARRT	Acquisition Requirements Roadmap Tool
ATO	Authority to Operate
B2B	Business-2-Business
CAC	Common Access Card
CAP	Cloud Access Point
CCEVS	Common Criteria Cybersecurity Evaluation and Validation Scheme
CDI	Covered Defense Information
CE	Computer Environment
CDRL	Contract Data Requirement List
CIO	Chief Information Officer
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CMMC	Cybersecurity Maturity Model Certification
CMR	Contractor Manpower Reporting
CNSSI	Committee on National Security Systems Instruction
CONUS	Continental United States (excludes Alaska and Hawaii)
CO	Contracting Officer(s)
COR	Contracting Officer Representative
COTR	Contracting Officer's Technical Representative

CS	Contract Specialist
CSP	Cloud Service Provider
CSSP	Cyber Security Service Provider
CUI	Controlled Unclassified Information
DA	Days After
DACA	Days After Contract Award
DAD-A	Deputy Assistant Director for Acquisition
DC3	DoD Cyber Crime Center
DD Form 254	Department of Defense Contract Security Requirement List (if applicable)
DB	Design-Build
DBB	Design-Bid-Build
DFARS	Defense Federal Acquisition Regulation Supplement
DHA	Defense Health Agency
DISA	Defense Information System Agency
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DSAs	Data Sharing Agreements
DSAA	Data Sharing Agreement Application
DMZ	Demilitarized Zone
DoDM	Department of Defense Manual
DoW	Department of War
DPCLO	DHA Privacy and Civil Liberties Office
DUA	Data Use Agreement
eMSM	Enhanced Multi-Service Markets
EULA	End User License Agreement
EVM	Earned Value Management
FAR	Federal Acquisition Regulation
FCI	Federal contract information
FE	Facilities Enterprise
FedRAMP	Federal Risk Authorization and Management Program
FISMA	Federal Information Security Modernization Act
FRCS	Facility Related Control Systems
FSO	Facilities Security Officer
HA	Health Affairs
HIPAA	Health Insurance Portability and Accountability Act
HCA	Head of the Contracting Activity
HIT	Health Information Technology
IGCE	Independent Government Cost Estimate
IA	Information Assurance
IO	Initial Outfitting
I/O	In/Out Processing Portal
IPv	Internet Protocol Version
IS	Information System
ISP	Internet Service Provider
IT	Information Technology

ISCM	Information Security Continuous Monitoring
IV&V	Independent Verification & Validation
MedCOI	Medical Community of Interest
MHS	Military Health System
MIL-STD	Military Standard
MTFs	Military Treatment Facilities
NCR	National Capitol Region
NDA	Non-Disclosure Agreement
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NLT	No Later Than
OCONUS	Outside Continental United States (includes Alaska and Hawaii)
ODC	Other Direct Costs
OPM	Office of Personal Management
OSD	Office of the Secretary of Defense
P-ATO	Personal Authorization to Operate
P&R	Personnel and Readiness
PGI	Procedures, Guidance and Information
PDT	Project Delivery Team
PHI	Protected Health Information
PII	Personally Identifiable Information
PIT	Platform Information Technology
PK	Public Key
PKI	Public Key Infrastructure
POA&M	Plan of Action and Milestones
POC	Point of Contact
PMO	Program Management Office
PoP	Period of Performance
PP	Personal Property
PPSM	Ports, Protocols, and Services Management
PRS	Performance Requirements Summary
PSP	Personnel Security Program
PWS	Performance Work Statement
QA	Quality Assurance
QAP	Quality Assurance Program
QASP	Quality Assurance Surveillance Plan
QC	Quality Control
QCP	Quality Control Plan
RFP	Request for Proposal
RFQ	Request for Quotation
RMF	Risk Management Framework
SAS	Statistical Analysis System
SP	Special Publication
SPRS	Supplier Performance Risk System
SRM	Sustainment, Restoration and Modernization
SRG	Security Requirements Guides

STIG	Security Technical Implementation Guides
TOS	Terms of Service
US	United States
UFC	Unified Facilities Criteria
VPN	Virtual Private Network
XML	Extensible Markup Language

2.3 Applicable Publications, DHA Administrative Instructions (AI), etc.

PART 3

3. GOVERNMENT FURNISHED PROPERTY, EQUIPMENT, AND SERVICES

3.1 Services:

The Government:

☒ **Will NOT** provide Government Furnished Services in support of this contract/task order. As a result, this paragraph is Not Applicable.

☐ **WILL** provide Government Furnished Services required in support of this contract/task orders. These Services are described below:

3.2 Facilities:

The Government:

☒ **Will NOT** provide Facilities in support of this contract/task order. As a result, this paragraph is Not Applicable.

☐ **WILL** provide Facilities in support of this contract/task orders. The Government provided Facilities are described below:

3.3 Utilities:

The Government:

☒ **Will NOT** provide Utilities in support of this contract/task order. As a result, this paragraph is Not Applicable.

☐ **WILL** provide Utilities in support of this contract/task orders. The Government provided Utilities are described below:

3.4 Equipment:

The Government:

☒ **Will NOT** provide Equipment in support of this contract/task order. As a result, this paragraph is Not Applicable.

☐ **WILL** provide Equipment in support of this contract/task orders. The Government provided Equipment is described below:

3.4.1 Procurement Integrated Enterprise (PIEE), GFP Module Application:

The Contractor shall be responsible for obtaining and maintaining access, training and successful operation of the PIEE/GFP Module application for the entirety of the contract/task order PoP. The PIEE GFP Module application is located at the following website: https://wawf.eb.mil/piee-landing/. Access to PIEE/GFP Module application training materials and in-depth information applicable to the Contractor's responsibilities regarding GFP can be found at the following website: https://dodprocurementtoolbox.com/.

Contracting Office Responsibilities:

The Contracting Office shall ensure close coordination and validation of the GFP items with the COR and DHA Accountable Property Officer prior to uploading the GFP Attachment into the PIEE/GFP Module. At the time GFP is anticipated and identified, the Government will upload the GFP Attachment into the PIEE/GFP Module. It is the Contracting Office's responsibility to prepare, upload and maintain the GFP Attachment in the PIEE/GFP Module in accordance with the GFP Attachment instructions provided at the DoD Procurement Toolbox. The CO and COR

shall manage and keep an inventory of any GFP associated with contract/task orders awarded through DHA, in accordance with applicable FAR Part 45, DoD FAR Supplement (DFARS) 245 with respective clauses, DHA AI 095 and PD 45-01 following the change in disposition of items listed on that PIEE/GFP Module Attachment.

The contracting office will also review, acknowledge, reject and/or approve shipment orders provided by the Contractor as appropriate. Functional roles can be determined within the Contracting Office and requested within the PIEE/GFP Module system.

Contractor Responsibilities:

A key Contractor responsibility is to work with the CO and COR to ensure the PIEE/GFP Module data, to include the PIEE/GFP Attachment, provides a timely, complete and accurate accounting of the GFP applicable to the contract/task order. Contractors are required to report the receipt of any GFP shipped to them, regardless of whether it is listed on the GFP Attachment for their contract. Similarly, Contractors are required to utilize the GFP Module application in conjunction with the shipment of GFP to the Government, or in reporting Property Loss of GFP issued (such as destruction or loss). Discrepancies or disputes regarding property shipped to or shipped from the Contractor must be reported via the GFP Module application, with the CO having authority over final designation of status.

The Contractor shall report, on a semi-annual basis, 100% inventories, reconciliations, and final disposition of GFP provided by the Government. Final invoices will not be paid pending GFP reconciliation. Contractors shall be aware of and ensure compliance with applicable FAR Part 45, DFARS 245 and 252.245, Defense Pricing and Contracting Policies, Procurement Integrated Enterprise Environment Standards, DHA Administrative Instruction 094 and DHA Guidance.

3.5 Materials:

The Government:

☒ **Will NOT** provide Materials in support of this contract/task order. As a result, this paragraph is Not Applicable.

☐ **IS** providing Materials in support of this contract/task orders. The Government-provided Materials are described below:

PART 4

4. CONTRACTOR FURNISHED ITEMS

4.1 Services:

The Contractor:

☐ **Will NOT** provide Contractor Furnished Services in support of this contract/task order. As a result, this paragraph is Not Applicable.

☒ **WILL** provide Contractor Furnished Services required in support of this contract/task orders. These Services are described below:

See PART 5.0 Specific Tasks

4.2 General:

The Contractor shall furnish all supplies, equipment, facilities and services required to perform work listed under Section 5 of this PWS.

4.3 Secret Facility Clearance: n/a

4.4 Materials: n/a

4.5 Equipment: n/a

4.6 Facilities: n/a

PART 5

5. SPECIFIC TASKS

5.1 Task 1: Software Maintenance

(FFP) The Contractor shall provide software licenses and maintenance for the licenses and templates listed below:

- Twelve (12) eCTD Publishing User Licenses
- Fifty (50) named eCTD Reviewing User Licenses (concurrent users)
- eCTD FDA Template

Licensing shall also include:

- The ability to perform hyperlinking within the publishing application
- The ability to do submission validation
- Validation Test scripts for the initial version and future versions of both eCTD Publishing software and eCTD Reviewing software

5.2 Task 2: Consulting and Technical Support Services

(Reimbursable) Consulting and Technical Support services requested shall include:

Standard eCTD Software Project Management:

The Contractor shall work collaboratively with the eIT PMO staff on remediation of network security vulnerabilities discovered during evaluation testing to achieve a secure software installation which is required to maintain the software on a Department of War (DoW) network. The Contractor shall provide necessary support and communication to schedule and provide all services.

Technical and Regulatory Services:

The Contractor shall provide technical support for installation, upgrades, and validation support for all software maintained under this contract on an as-needed basis. Technical support services are required for but not limited to:

- Project Management
- Regulatory Services
- Installation of eCTD software products
- Pre-installation and installation testing
- Validation support – scripts included
- eCTD Software Upgrade Support

Installation, Testing, Configuration, Migration, Validation, etc.:

The Contractor shall work collaboratively with eIT PMO staff on the installation, configuration, upgrades and data migration of eCTD software products, modules, and data into two (2) computing environments (test and production) in a data center or in a cloud environment. This will include the development/modification of installation instructions to allow the products to function within the parameters specified for DoW installations.

The Contractor shall provide technical support and documentation for testing and validation of the products. Documents to be generated, authored/updated, and provided shall include the following on an as needed basis:

a. Master Validation Plan (MVP)
b. Design Specifications
c. Validation Test Plan for Installation Qualification (IQ) based on vendor provided templates

d. Validation source book for Installation Qualification (IQ)/Operational Qualification (OQ)/Performance Qualification (PQ)
e. Modification of standard IQ test scripts for eIT PMO installation
f. System Configuration guide
g. Work instructions and process flow
h. Documents should be provided in Microsoft Word format and be updated for the software version that is being supported

5.3 Task 3: Training Consulting and Technical Support Services

The Contractor shall:

- Provide a list of training courses offered (private onsite or online) with associated costs for eCTD products. The training is to be scheduled on an as-needed basis, at a mutually agreed time. The cost should be priced per class.
- Provide descriptions and complete pricing to include estimated billable hours for available training options (course trainings, tailored training, and/or mentoring) to allow eIT PMO to compare and select from courses, vendor-provided training, or mentoring in advance
- Provide training that includes any new functionality, refresher training, and new modules that become available or are required
- Accommodate request for training or mentoring within 30 calendar days after notification from the Government
- Provide remote mentoring for the development, programming and configuration and deployment of the eCTD product
- Provide certified implementation experts to conduct mentoring. The mentoring provided should be a combination of custom training in conjunction with hands on environment specific consulting.

The Contractor shall provide a list of training courses available with costs and cost of all training materials. Training courses shall include but may not be limited to:

- Standard eCTD Publisher Training
- Advanced eCTD Publisher Training
- Administrator Training
- eCTD Reviewer Training
- Training materials shipping expense (if required)
- Daily / Ad hoc training with daily rate

The Government intends to utilize a “Plugged” Not-to-Exceed (NTE) amount for all Training ODCs – See ODC Matrix Below. This plugged value is inclusive of all items outlined in this PWS Section.

ODC Matrix: Base Period & All Option Periods

Contract Period	Training ODC Plugged Values
Base Period	$8,000.00
Option Period 1 (OP1)	$8,240.00
Option Period 2 (OP2)	$8,487.20
Option Period 3 (OP3)	$8,741.82

Option Period 4 (OP4)	$9,004.07
52.217-8 (6-month period)	$4,637.10

The Government will request training based on frequency and need and will coordinate with the Contractor when training requirements are required. Basic training requirements are outlined in PWS Section 5.3 (Task 3), and the contractor is required to provide basic training pricing (if not separately priced elsewhere), and these prices will be utilized to request training and fund it as required throughout the life of this contract.

5.4 Task 4: Travel

The Government intends to utilize a "Plugged" Not-to-Exceed (NTE) amount for all Travel ODCs – See ODC Matrix Below. This plugged value is inclusive of all travel related to items outlined in PWS Section 5.3 (Task 3: Training Consulting and Technical Support Services).

ODC Matrix: Base Period & All Option Periods

Contract Period	Travel ODC Plugged Values
Base Period	$3,000.00
Option Period 1 (OP1)	$3,000.00
Option Period 2 (OP2)	$3,000.00
Option Period 3 (OP3)	$3,000.00
Option Period 4 (OP4)	$3,000.00
52.217-8 (6-month period)	$1,500.00

Arrangements for and costs of all travel, transportation, meals, lodging, and incidentals are the responsibility of the Contractor. Travel costs shall be incurred and billed in accordance with FAR Part 31. All travel requires Government prior approval/authorization. Costs for these expenses will be reviewed, certified and approved by the COR in advance. Contractor shall submit travel requests with estimated costs to the COR NLT fifteen (15) calendar days prior to travel. All travel and transportation shall utilize commercial sources and carriers provided the method used for the appropriate geographical area results in reasonable charges to the government. The Government will not pay for business class or first-class travel. Lodging and meals shall be reimbursed in accordance with regulations defined in FAR PART 31.

PART 6

6. INFORMATION TECHNOLOGY & SECURITY

6.1 All work under this contract is unclassified.

6.2 The TIER 2 levels and position sensitivity designation for positions under this contract is (Requirement must be checked in order to be a requirement for this PWS):

6.2.1 TIER II: Non-critical sensitive position.

6.3 Personally Identifiable Information (PII)/Protected Health Information (PHI), Procurement, and Federal information requirements:

6.3.1 Data Sharing Agreements (DSAs): Contractors requiring access to PII, which includes PHI, or access to de-identified data, are subject to the DHA Privacy and Civil Liberties Office (DPCLO) (Privacy Office) Data Sharing Program. This program requires DHA to enter into DSAs with parties outside the MHS who use or create MHS data. A DHA contract may use the term Data Use Agreement (DUA) rather than DSA. DSAs assure that outside parties protect MHS data in accordance with the Privacy Act and the HIPAA Rules. To apply for a DSA, the Contractor submits a Data Sharing Agreement Application (DSAA) to the DHA DPCLO. The Contractor submits the DSAA even if a subcontractor will be the party accessing MHS data. After review and approval of the DSAA, the Privacy Office provides a DSA to the Contractor for execution.

6.3.2 Processing Procurement Sensitive Information: All individuals shall seek guidance from the CO regarding the coordination of documents, dissemination, and transmission of procurement sensitive information. Procurement sensitive information shall not be transmitted electronically unless encryption is utilized. Depending on a particular procurement, other restrictions may apply.

6.4 Training:

6.4.1 Contractor employees performing cybersecurity/cyberspace functions shall comply with the following requirements: n/a

6.4.2 User requirements: All Contractor employees that require access to DHA IT must comply with the requirements of DHA-Procedural Instruction 8140.01, Acceptable Use of DHA IT, to include those contract employees with privileged access.

6.5 Cybersecurity Requirements for Non-DoW IT or Covered Contractor IS: n/a

6.5.1 The Contractor shall mitigate supply chain risk to the Government by complying with DFARS 252.239-7018 and only utilizing unified capability equipment identified on the DODIN Unified Capabilities Approved Products List (https://aplits.disa.mil/processAPList), unless granted a waiver in accordance with DODI 8100.04, DOD Unified Capabilities (UC).

6.6 Risk Management Framework (RMF) for DoW IT:

All IS, Platform Information Technology (PIT) and IT Services or Products under this requirement, that receive, transmit, store, or process nonpublic Government data must be accredited in accordance with DoDI 8510.01, Risk Management Framework (RMF) for DoD IT and comply with annual Federal Information Security Modernization Act (FISMA) security control testing. IS and PIT systems must be categorized in accordance with Committee on National Security Systems Instruction (CNSSI) 1253, implement a corresponding set of security controls from the NIST SP 800-53, and use assessment procedures from NIST SP 800-53A with additional DoW-specific assignment values, overlays, implementation guidance, and assessment procedures as required.

6.6.1 All systems subject to RMF must present evidence of authorization in the System Security Plan, Security Assessment Report) a Plan of Action and Milestones (POA&M) and authorization decision document or show that the system has a DoW RMF or equivalent DoW Component PIT system accreditation decision that is current within three years within five (5) business days of CO request. Evidence of FISMA compliance must be presented in the form of a POA&M. Systems must have and maintain an Authority to Operate (ATO) or Authority to Operate with Conditions (ATO-C) by contract award.
6.6.2 The Contractor shall implement security controls in accordance with NIST implementation and validation requirements specified in the NIST SP 800-37 Risk Management Framework (RMF) and DoDI 8510.01, Risk Management Framework (RMF).
6.6.3 The Contractor shall configure the information system in accordance with Defense Information Agency (DISA) Security Requirements Guides (SRGs) and security technical implementation guides (STIGs).
6.6.4 The Contractor shall ensure that the information system conforms to the requirements of DoDI 8551.01 "Ports, Protocols, and Services Management (PPSM)."
6.6.5 The Contractor shall ensure that the information system shall authenticate all entities as specified in DoDI 8520.03 "Identity Authentication for Information Systems" prior to granting access.
6.6.6 The Contractor shall Public Key (PK) enable the information system, implementing digital signature and encryption requirements specified in DoDI 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling."
6.6.7 The Contractor will be responsible for compliance with the Joint Force Head Quarters – Department of Defense Information Network issuances and IA Vulnerability Management (IAVM) issuances by ensuring that the issuances are assessed, implemented and maintained throughout development and sustainment in accordance with specified timelines.
6.6.8 The Contractor shall support reciprocity, by providing all directed information in NIST security documents to the Government.
6.6.9 The Contractor shall implement system level protection and detection capabilities that are consistent with their contract for NIST Security requirements that meet DoW and DHA Cybersecurity Architectures.
6.6.10 Cyber Incident Reporting Requirement: The Contractor shall comply with the incident management requirements of Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01B, "Cyber Incident Handling Program".
6.6.11 Information security continuous monitoring (ISCM): ISCM is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. ISCM is a critical part of the risk management process to ensure that IS and PIT operations remain within an acceptable level of risk despite any changes that occur. The Contractor shall maintain ongoing monitoring, analysis and incident response procedures for all ARRT and PIT systems under this requirement in accordance with NIST SP 800-137.
6.6.12 The Contractor shall mitigate supply chain risk to the Government by complying with DFARS 252.239-7018 and only utilizing unified capability equipment identified on the DODIN Unified Capabilities Approved Products List (https://aplits.disa.mil/processAPList), unless granted a waiver in accordance with DODI 8100.04, DOD Unified Capabilities (UC).

6.7 Facility Related Control Systems: RESERVED

6.8 System Communications: RESERVED

6.9 MHS Demilitarized Zone (DMZ) Medical Community of Interest (MedCOI) Business-to-Business (B2B) Gateway

6.9.1 If there is an external system connection to a DoW IS required, then the Contractor shall, in accordance with contract requirements, connect to the DHA B2B Gateway via a Contractor procured Internet Service Provider (ISP) connection.

6.9.2 The Contractor shall assume all responsibilities for establishing and maintaining their connectivity to the B2B Gateway. This shall include acquiring and maintaining the circuit used to connect to the B2B Gateway and the acquisition of a Virtual Private Network (VPN) device maintenance agreement and license compatible with the MHS VPN device. The list of compatible devices are detailed in the DHA B2B/MedCOI Gateway questionnaire.

6.9.3 The Contractor shall submit a completed current version of the DHA B2B Gateway questionnaire to their Contracting Officer or COR within ten (10) calendar days after new requirements have been provided to the Contractor.

6.9.4 The Contractor shall provide information specific to their connectivity requirements, proposed path for the connection and last mile diagram.

6.10 Contractor Provided IT Infrastructure

6.10.1 Platforms shall support HyperText Transfer (Transport) Protocol (HTTP), HyperText Transfer (Transport) Protocol Secure (HTTPS), web-derived Java Applets, and Secure File Transfer Protocols (SFTPs) (e.g., STFP, Secure Socket Layer/Transport Layer Security), and all software that the Contractor proposes to use to interconnect with DoW facilities.

6.10.2 The Contractor shall configure their networks to support access to Government systems (e.g., configure ports and protocols for access).

6.10.3 The Contractor shall provide full time connections to a TIER 1 or TIER 2 ISP. Dial-up ISP connections are not acceptable. All IP addresses need to be publicly routable. Private address space using Network Address Translation will not be permitted.

6.10.4 The Contractor shall maintain a valid maintenance contract and pertinent licenses for all devices connecting to the MHS B2B Gateway.

6.11 System Authorization Access Request (SAAR), Defense Department (DD) Form 2875

6.11.1 The Contractor shall submit the most current version of DD Form 2875, "System Authorization Access Request (SAAR), in accordance with CO guidance for all Contractors that use the DoW Gateways to access Government IT systems and/or DoW applications shall. A DD Form 2875 shall be completed for each Contractor employee who will access any system and/or application on a DoW network. The DD Form 2875 shall clearly specify the system and/or application name and justification for access to that system and/or application.

6.11.2 The Contractor shall submit the completed DD Form 2875 to the DHA IT Security for verification of Tier I or Tier II Designation. The DHA Personnel Security will verify that the Contractor employee has the appropriate background investigation completed or a request for background investigation has been submitted to the Office of Personal Management (OPM). Acknowledgment from OPM that the request for a background investigation has been received and that an investigation has been scheduled will be verified by the DHA Personnel Security prior to access being approved.

6.11.3 Upon approval, DHA will notify the user of the ID and password via secure/encrypted e-mail upon the establishment of a user account. User accounts will be established for individual use and may not be shared by multiple users or for system generated access to any DoW application. Misuse of user accounts by individuals or Contractor entities will result in termination of system access for the individual user account.
6.11.4 The Contractor shall conduct a monthly review of all Contractor employees who have been granted access to DoW IS networks to verify that continued access is required.
6.11.5 The Contractor shall provide the DHA DPCLO with a report of the findings of their review by the 10th calendar day of each month following the review. Reports identifying changes to Contractor employee access requirements shall include the name, DoW ID number from CAC, Company, IS/network for which access is no longer required, and the date access will be terminated.

6.12 MHS Systems Telecommunications

6.12.1 The primary communication links shall be via encrypted tunnels (i.e., Secure Internet Protocol (IPSEC), GetVPN, or Secure Socket Layer) between the Contractor's primary site and the MHS B2B Gateway.
6.12.2 The Contractor shall place the VPN appliance device outside the Contractor's firewalls and shall allow full management access to this device (e.g., in router access control lists) to allow Central VPN Management services provided by DHA or other source of service as designated by the MHS to remotely manage, configure, and support this VPN device as part of the MHS VPN domain.
6.12.3 The Contractor shall procure and configure for operation an auxiliary VPN device for backup purposes to minimize any downtime associated with problems of the primary VPN.
6.12.4 The Contractor shall send devices to the MHS VPN management authority (e.g., DHA) via postage paid and include prepaid return shipping arrangements for the devices(s).
6.12.5 The MHS VPN management authority (e.g., DHA) will remotely configure and manage the VPN appliance once installed by the Contractor.
6.12.6 The Contractor shall be responsible for the maintenance and repair of Contractor procured VPN equipment.
6.12.7 The Government will be responsible for the troubleshooting of VPN equipment.

6.13 Establishment of Telecommunications

6.13.1 Telecommunications shall be established with the MHS through coordination with DHA.
6.13.2 The Contractor and DHA Program Office shall identify their requirement(s) for the establishment of telecommunications with the MHS and/or other Government entities.
6.13.3 The DHA/MedCOI B2B Gateway Questionnaire (provided by DHA) identifies the required telecommunication infrastructure between the Contractor and the MHS systems. This includes all Wide Area Network, Local Area Network, VPN, Web DMZ, and B2B Gateway access requirements.
6.13.4 The Contractor shall complete their applicable portion of the questionnaire and shall return it to the DHA designated POC for review and approval.
6.13.5 The Contractor shall, Upon Government request, provide technical experts to provide any clarification of information provided in the questionnaire. DHA will review and process the questionnaire when it is accepted.
6.13.6 DHA will coordinate any requirements for additional information with the POC and schedule any meetings required to review the Questionnaire. Upon approval of the Questionnaire, DHA will coordinate a testing meeting with appropriate stakeholders.

6.13.7 DHA will notify the Contractor POC of the meeting schedule. The purpose of the testing meeting is to complete a final review of the telecommunication requirements and establish testing dates.

6.14 Contractors Located On Military Installations

6.14.1 The Contractor(s) shall coordinate/obtain the connections with the local MTFs/ Enhanced Multi-Service Markets (eMSMs) and Base/Post/Camp communication personnel located on a military installation who require direct access to Government systems.

6.14.2 These connections will be furnished by the Government.

6.14.3 Contractors located on military installations that require direct connections to their networks shall provide an isolated IT infrastructure. They shall coordinate with the Base/Post/Camp communications personnel and the MTF/eMSM to obtain approval for a Contractor-procured circuit prior to installation to ensure the Contractor is within compliance with the respective organizational security policies, guidance and protocols.

Note: In some cases, the Contractor may not be allowed to establish these connections due to local administrative/security requirements.

6.14.4 The Contractor shall be responsible for all security certification documentation as required to support DoW IA requirements for network interconnections.

6.14.5 The Contractor shall provide, on request, detailed network configuration diagrams to support IA accreditation requirements.

6.14.6 The Contractor shall comply with IA accreditation requirements. All network traffic shall be via Transmission Control Protocol/Internet Protocol using ports and protocols in accordance with current Service security policy. All traffic that traverses MHS and/or military Service Base/Post/Camp security infrastructure is subject to monitoring by security staff using Intrusion Detection Systems.

6.15 Cybersecurity Maturity Model Certification (reference DFARS 252.204-7012)

Cybersecurity Maturity Model Certification (CMMC) **level 1 certification** is required with "self-assessment" required prior to award. CMMC Program requirements apply to Contractors who will process, store, or transmit Federal Contract Information (FCI – information NOT intended for public release) or Controlled Unclassified Information (CUI – information that requires safeguarding and is subject to dissemination controls).

The contractor shall register at: https://piee.eb.mil/xhtml/unauth/home/login.xhtml and obtain a "SPRS Cyber Vendor User" role to enter CMMC assessment information. Offerors can learn more by viewing these training videos: https://www.sprs.csd.disa.mil/ and watching "CMMC Assessment Tutorial" and "Affirming Official Tutorial for CMMC." Self-assessment is good for 180 days. After 180 days, self-assessment will expire. **A copy of the self-assessment, with score, shall be submitted with the proposal**.

For level 2 and 3 certifications contractors will need to obtain third-party certification. Cyber AB is the official accreditation body of the CMMC: https://cyberab.org.

Contractors that use external cloud service providers that store, process, or transmit any covered defense information shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the FedRAMP Moderate baseline and comply with DFARS 252.204-7012. More information can be obtained at:

https://dodcio.defense.gov/Portals/0/Documents/CMMC/FedRAMP-AuthorizationEquivalency.pdf and https://www.fedramp.gov/.

Additional information regarding CMMC can be obtained at: https://dowcio.war.gov/CMMC/.

Additional Helpful Links*:

CIO – Cybersecurity Maturity Model Certification: https://dodcio.defense.gov/CMMC/
CIO – About CMMC: https://dodcio.defense.gov/CMMC/about/
Cyber AB – What is CMMC: https://cyberab.org/What-is-CMMC
Cyber AB – CMMC Ecosystem: https://cyberab.org/CMMC-Ecosystem/What-is-CMMC
CMMC 2.0 Details and Links to Key Resources: https://business.defense.gov/Programs/Cyber-Security-Resources/CMMC-20/
CMMC – Compliance | Google Cloud: https://cloud.google.com/security/compliance/cmmc
What is CMMC? 3 Levels Every DoD Contractor Needs to Know: https://www.youtube.com/watch?v=cPqzoj9Jnl4&t=400
Cybersecurity Maturity Model Certification – Amazon Web Services (AWS): https://aws.amazon.com/compliance/cmmc/
Pentagon Needs More CMMC Third-Party Assessors to Increase Compliance Rates, Slash Waits & Costs—Experts Weigh in: https://www.executivegov.com/articles/cmmc-dow-cybersecurity-c3pao-cio
What Federal Contractors Need to Know About CMMC – The Coalition for Government Procurement: https://thecgp.org/what-federal-contractors-need-to-know-about-cmmc/
CMMC Third Party Assessor Organizations (C3PAO) — CMMC Marketplace: https://cmmcmarketplace.org/c3pao
Defense Contract Management Agency > DIBCAC: https://www.dcma.mil/DIBCAC/

***Links/References to any specific product, service, or method does not constitute an implied or expressed recommendation or endorsement by the Government.**

PART 7

7. ATTACHMENTS/TECHNICAL EXHIBIT LISTING

Overview

The eCTD Publisher System is intended for use by eIT PMO customers/user base for preparation and lifecycle maintenance of electronic regulatory submissions originating from the Army Office of the Surgeon General (OTSG) sponsored investigational product development. The critical function of the system is the ability to generate electronic regulatory submissions. In addition, the system shall have the ability to automate workflow steps required to manage preparation of electronic submissions for submission to regulatory agencies (e.g., FDA) in the US only.

The eCTD publishing system shall be used for:

- Preparation and lifecycle maintenance of electronic regulatory submissions.
- Greater efficiency within regulatory submissions.
- A higher level of compliance with applicable regulations.

The eCTD publishing system shall have the ability to:

- Scale to support increases in the number of electronic regulatory submissions resulting from expanding clinical trial activities, including multiple concurrent preparation and review activities, without degradation of system performance.
- Provide seamless access to third parties (e.g., external regulatory reviewers, CRO's, etc.).
- Integrate the eCTD publishing system with other key DHA systems (e.g., Open Text – Content Server).
- The eCTD software shall be capable of interfacing with OpenText Content Server 22.4 and current releases. The eCTD software must support Microsoft Windows Server 2019 R2 (64-bit) operating system and newer. This is a designated go, no-go requirement under RFP Technical Approach.
- The eCTD software shall also meet U.S. Food & Drug Administration (FDA) 21 CFR Part 11 requirements. This is a designated go, no-go requirement under RFP Technical Approach.
- The eCTD Software shall be able to be installed on-premise and in the cloud in accordance with CMMC standards.
- The eCTD system will be managed and maintained by the eIT PMO.
- The technical support services must include supporting the import of existing eCTD submissions and their full lifecycles from the existing eCTD publishing system. This software is also part of a suite of FDA compliant products maintained by the eIT PMO.
- The eCTD software must be able to be installed and configured in accordance with cybersecurity best practices to reside on the DHA network. The vendor providing the software license and maintenance must support the Government with any technical application modifications to ensure the Government can receive a Risk Management Framework (RMF) Authority to Operate (ATO).

***Directive**: FDA-compliant software products used for clinical trial research must support the stringent security controls and compliance with U.S. Food & Drug Administration 21 CFR Part 11 electronic records and signature requirements.*

PART 8
ATTACHMENT 1
PERFORMANCE REQUIREMENTS SUMMARY

Performance Objective (The Service required—usually a shall statement from Part 5)	**PWS Reference**	**Acceptable Quality Level (AQL)** (This is the maximum error rate. It could possibly be "Zero deviation from standard")	**Method of Surveillance**
Performance Requirements Summary (PRS) # 1 The Contractor shall provide software licenses and maintenance for the licenses and templates listed below: • Twelve (12) eCTD Publishing User Licenses • Fifty (50) named eCTD Reviewing User Licenses (concurrent users) • eCTD FDA Template Licensing shall also include: • The ability to perform linking within the publishing application • The ability to do submission validation • Validation Test scripts for the initial version and future versions of both eCTD Publishing software and eCTD Reviewing software	PWS Part 5 - 5.1	Provide as needed	100% inspection
PRS # 2 The Contractor shall work collaboratively with the eIT PMO staff on remediation of network security vulnerabilities discovered during evaluation testing to achieve a secure	PWS Part 5 - 5.2	Provide as needed	100% inspection

software installation which is required to maintain the software on a DoW network. The Contractor shall provide necessary support and communication to schedule and provide all services. The Contractor shall provide technical support for installation, upgrades, and validation support for all software maintained under this contract on an as-needed basis. Technical support services are required for but not limited to: • Project Management • Regulatory Services • Installation of eCTD software products • Pre-installation and installation testing • Validation support- scripts included • eCTD Software Upgrade Support The Contractor shall work collaboratively with eIT PMO staff on the installation, configuration, upgrades and data migration of eCTD software products, modules, and data into two (2) computing environments (test and production) in a datacenter or in a cloud environment. This will include the development/modification of installation instructions to allow the products to function within the parameters specified for Department of War installations. The Contractor shall provide technical support and documentation for testing and validation of the products.			

Documents to be generated, authored/updated, and provided shall include the following on an as needed basis: a. Master Validation Plan (MVP) b. Design Specifications c. Validation Test Plan for Installation Qualification (IQ) based on vendor provided templates d. Validation source book for Installation Qualification (IQ)/Operational Qualification (OQ)/Performance Qualification (PQ) e. Modification of standard IQ test scripts for eIT PMO installation f. System Configuration guide g. Work instructions and process flow h. Documents should be provided in Microsoft Word format and be updated for the software version that is being supported.			
PRS # 3 The Contractor shall: • Provide a list of training courses offered (private onsite or online) with associated costs for eCTD products. The training is to be scheduled on an as-needed basis, at a mutually agreed time. The cost should be priced per class. • Provide descriptions and complete pricing to include estimated billable hours for available training options (course trainings, tailored training, and/or mentoring) to	PWS Part 5 - 5.3	Provide as needed	100% inspection

allow eIT PMO to compare and select from courses, vendor-provided training, or mentoring in advance. • Provide training that includes any new functionality, refresher training, and new modules that become available or are required. • Accommodate request for training or mentoring within 30 calendar days after notification from the Government. • Provide remote mentoring for the development, programming and configuration and deployment of the eCTD product. • Provide certified implementation experts to conduct mentoring. The mentoring provided should be a combination of custom training in conjunction with hands on environment specific consulting. The Contractor shall provide a list of training courses available with costs and cost of all training materials. Training courses shall include but may not be limited to: • Standard eCTD Publisher Training • Advanced eCTD Publisher Training • Administrator Training • eCTD Reviewer Training • Training materials shipping expense (if required) • Daily/Ad hoc training with daily rate			

PART 8
ATTACHMENT 2
DELIVERABLE SCHEDULE

8.1 Delivery Address

All deliverables shall be submitted to the COR designated in the COR appointment letter and as directed by the COR upon award of the contract.

8.2 Method of Delivery

Electronic copies shall be delivered using Microsoft Office suite of tools (for example, MS WORD, MS EXCEL, MS POWERPOINT, MS PROJECT, or MS ACCESS format), unless otherwise specified by the COR. Electronic submission shall be made via email, unless otherwise agreed to by the COR.

8.3 Shipping

The Contractor shall use the U.S. Postal Service standard delivery for delivery of materials, equipment, or required hardcopy documents. The COR must approve all exceptions to this requirement.

8.4 Government Acceptance Period

The COR will have ten (10) business days to review draft deliverables and make comments. The Contractor shall have five (5) business days to make corrections. Upon receipt of the final deliverables, the COR will have two (2) business days for final review prior to acceptance or providing documented reasons for non-acceptance. Should the Government fail to complete the review within the review period the deliverable will become acceptable by default, unless prior to the expiration of the ten (10) business days the Government notifies the Contractor in writing to the contrary. The final submission should be deemed approved if the Government has not rejected it in 30 calendar days.

The COR will have the right to reject or require correction of any deficiencies found in the deliverables that are contrary to the information contained in the Contractor's accepted proposal. In the event of a rejected deliverable, the Contractor will be notified in writing by the COR of the specific reasons for rejection. The Contractor shall have five (5) business days to correct the rejected deliverable and return it per delivery instructions.

8.5 Deliverable/Delivery Schedule Table

A summary of deliverables follows. Copies are to be provided to the Government officials electronically.

(This technical exhibit lists any reports or documentation that is required as a deliverable, to include the frequency, # of copies, medium/format and who/where it is to be submitted. A deliverable is anything that can be physically delivered but may include non-physical things such as meeting minutes. Note: All PWS deliverables should be included in this exhibit.)

Deliverable	Frequency	Medium/Format	Submit To	Appliable To (PWS Ref.)
Deliverable 1: Quality Control Plan	Initial: NLT 30 DACA. Subsequent: Update as required.	Electronic	COR	1.10.1
Deliverable 2: Non-Disclosure Agreement	Initial: Signed statements are due for all personnel prior to performing any work. Subsequent: Update as required.	Electronic	COR	1.12.2
Deliverable 3: Monthly Progress Report	Initial: NLT 45 DACA. Subsequent: NLT 5th calendar day of each month.	Electronic	COR and CS	1.12.3
Deliverable 4: Monthly Project Burn Report	Initial: NLT 35 DACA. Subsequent: NLT 5th calendar day of each month.	Electronic	COR	1.12.3

PWS ATTACHMENT A
DHA CONTRACTOR NON-DISCLOSURE AGREEMENT ("AGREEMENT")
(DHA FORM 49)

I, _____ am an employee of, or an employee of a subcontractor to, _____ (Business Name), a contractor to the Defense Health Agency (DHA) under Contract No. _____ through Delivery Order No. (as applicable) _____.

I understand that, in my performance under this contract, I may have access to, or otherwise receive, sensitive or proprietary business, technical, financial, and/or source selection information belonging to the Government or other contractors. This information includes, but is not limited to, cost/pricing data, Government spend plan data, contractor technical proposal data, contractor trade secrets, independent government cost estimates, proposal and evaluation and source selection information, negotiation strategies and contractor data presented in negotiations, contracting plans, and statements of work. I agree not to discuss, divulge, or disclose any such information or data to any person or entity, except those persons directly involved, on behalf of the DHA, in the acquisition or contract action to which the protected information pertains, as identified to me by the DHA contracting officer. I acknowledge that the unauthorized disclosure, use or negligent handling of the information by me could cause irreparable injury to the owner of the information.

As used in this Agreement, sensitive information is an overarching term that also includes, but is not limited to, sensitive but unclassified information/data, Protected Health Information, For Official Use Only information/data, and Privacy Information. This includes information in routine Department of Defense payroll, finance, logistics, inventory, and personnel management systems. The loss of, misuse of, or unauthorized access to or modification of this information could adversely affect the national interest or the conduct of Federal programs or the privacy to which individuals are entitled under Section 552a of Title 5, as amended, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

I attest that I am aware of, and will comply with the standards for access, dissemination, handling, and safeguarding of the information to which I am granted access as cited in this Agreement and in accordance with the guidance provided to me relative to the specific category of information.

I understand that the United States Government may seek any remedy available to it to enforce this Agreement, including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement. Court costs and reasonable attorney fees incurred by the United States Government may be assessed against me if I lose such action. I understand that another business entity might file a separate claim against me if I have misused its proprietary information.

Sensitive, proprietary, confidential commercial, or source selection information/data will be handled in accordance with Government regulations, policies, and procedures. I understand that I will be required to sign a new NDA for the contract in which I am performing, on an annual basis, prior to the Government granting me access to such information. I further understand that my obligations under this Agreement continue indefinitely and are not limited by the signing of a new agreement or by the term of my employment as a Government contractor employee. I fully understand that information does not lose its protected nature due simply to the passage of time, and my obligation of non-disclosure continues unless and until the information clearly falls under categories a through d in the next paragraph.

The obligations imposed herein do not extend to information/data which:

a) is in the public domain at the time of receipt or it came into the public domain through no act of mine;
b) is disclosed with the prior written approval of the DHA designated Contracting Officer;
c) is demonstrated to have been developed by (Business Name) or me independently of disclosures made hereunder; and
d) is disclosed pursuant to court order, after notification to the DHA designated Contracting Officer;

In the event that I seek other employment, I will reveal to any prospective employer the continuing obligation in this Agreement prior to accepting any employment offer.

I have read this Agreement carefully and my questions, if any, have been answered to my satisfaction.

1. NAME OF EMPLOYEE OR SUBCONTRACTOR EMPLOYEE	**2. BUSINESS ENTITY**
3. SIGNATURE OF EMPLOYEE OR SUBCONTRACTOR EMPLOYEE	**4. DATE (YYYYMMDD)**
5. WITNESS SIGNATURE	**6. DATE (YYYYMMDD)**

(End of DHA CONTRACTOR NON-DISCLOSURE AGREEMENT – DHA FORM 49)

(End of PWS)