STATEMENT of WORK

1. TASK ORDER TITLE

Cancer Therapy Evaluation Program Informatics & Computer Support

2. BACKGROUND

The National Cancer Institute (NCI) is the federal government's principal agency for cancer research and training. Established under the National Cancer Institute Act of 1937, NCI is part of the National Institutes of Health (NIH), one of the 11 agencies that make up the Department of Health and Human Services (HHS).

NCI's mission is to lead, conduct, and support cancer research across the nation to advance scientific knowledge and help all people live longer, healthier lives. As the leader of the cancer research enterprise, collectively known as the National Cancer Program, and the largest funder of cancer research in the world, NCI manages a broad range of research, training, and information dissemination activities that reach across the entire country.

The initial CTEP Informatics and Computer Support contract was awarded in 1996 in response to the recommendations to design, develop, and implement innovative data collection systems, management tools, and internal information storage as well as communication methods and systems. This system is termed the Cancer Therapy Evaluation Program – Enterprise System (CTEP-ESYS). CTEP-ESYS enhancement and integration decisions are based on the following principles:

- Provide a cost-effective approach to address administrative, scientific, and regulatory concerns
- Provide reliable clinical results and toxicity data
- Enable a shift in focus from administrative tasks to science for the scientists and physicians
- Improve patient/trial safety
- Ensure the security and confidentiality of proprietary and patient information
- Eliminate data redundancy throughout the oncology community
- Empower personnel to make educated decisions by improving access to quality and timely data

Today, the CTEP-ESYS is a highly integrated enterprise system consisting of approximately 29 applications and services. While some applications are available to clinical trial staff and are designed to facilitate data submission as required by federal regulation, most of the applications are accessible only by NCI/NIH personnel (and approved Contractors) to assist in achieving the scientific goals of CTEP and the NCI while bringing operating efficiencies to new and future business practices.

Note: A Glossary of Acronyms is provided in Appendix 2.

3. OBJECTIVE

The objectives of this Statement of Work (SOW) are to acquire services to provide enhancement, re-engineering, maintenance, and integration support for CTEP-ESYS including work involving other systems supported or utilized throughout the NCI including, but not limited to, the Clinical Trials Support Unit (CTSU), Enterprise System and Clinical Trials Monitoring Service (CTMS), Division of Cancer Treatment and Diagnosis (DCTD), Division of Cancer Prevention (DCP), the Coordinating Center for Clinical Trials (CCCT), and the Center for Biomedical Informatics and Information Technology (CBIIT), which may result in integration with the CTEP-ESYS.

4. SCOPE OF WORK

The scope of services to be provided fall under the following NITAAC CIO-SP3 task areas:

- Task Area 1: IT Services for Biomedical Research, Health Sciences, and Healthcare
- Task Ares 5: IT Operations and Maintenance
- Task Area 6: Integration Services
- Task Area 7: Critical Infrastructure Protection and Information Assurance
- Task Area 8: Digital Government
- Task Area 9: Enterprise Resource Planning
- Task Area 10: Software Development

The Contractor shall modify and/or enhance CTEP-ESYS applications and infrastructure as needed to address evolving scientific, regulatory, and administrative needs.

5. TASKS

The Contractor shall perform the following tasks:

- Task 1 Task Order Management
- Task 2 IT Infrastructure and System Security
- Task 3 Operations and Maintenance
- Task 4 Information Management

5.1 TASK 1 – TASK ORDER (TO) MANAGEMENT

Effective Task Order (TO) management is essential to the success of the Contract.

The Contractor shall:

1. Provide the technical and functional activities necessary for the management of this SOW, including oversight of all tasks provided by Contractor personnel, including Subcontractors, to satisfy the requirements identified in this SOW.
2. Assume responsibility to meet the cost, performance, and schedule requirements through the task execution.
3. Meet with CTEP personnel within two hours' notice at either NCI or Contractor meeting location or by use of available technologies (e.g., WebEx, Microsoft Teams).

5.2 TASK 2 – IT INFRASTRUCTURE AND SYSTEM SECURITY

The work to be performed under this task relates to the implementation and upkeep of CTEP-ESYS data center components, protection of the data and respective applications from internal and external threats and applying effective and efficient mechanisms to restore CTEP operations after a security incident.

5.2.1 Data Center Services

The Contractor shall maintain the CTEP applications within the NIH or NCI data center (or NCI managed cloud environment if applicable) following the Data Center hosting requirements at all times. These requirements may include but are not limited to the following:

5.2.1.1 Requirements and service

1. Notify data center of any changes in needs or requirements.
2. Provide current contact and escalation information for the Federal Sponsor of the application and Technical Project Lead.
3. Submit service requests as per data center policy.
4. Call the on-call phone number for critical emergencies, and not for general support.

5.2.1.2 Software

1. Provide and maintain all software that is necessary for CTEP-ESYS environment or service that is not provided by the data center.
2. Use software that has vendor or community support per HHS policy.
3. Build and/or maintain stable and secure applications or services.
4. Document CTEP-ESYS equipment configuration and specifications.
5. Manage all CTEP-ESYS equipment including shut down and restarts.
6. Provide remediation for all CTEP-ESYS application and service issues.
7. Perform all application deployments.

5.2.1.3 Facility Safety

1. Shut down any CTEP-ESYS equipment if it is detected that it presents a hazard, is doing harm to, or has harmed the facility unless said equipment is provided by NIH or CBITT.
2. Adhere to rules of behavior specified in the NIH or NCI Data Center Policy and Work Rules document.
3. Adhere to the NIH or NCI Data Center Infrastructure Guidelines for infrastructure rack, wiring, tools and labeling, and naming standards within the Data Center.

5.2.2 System Security

The Contractor shall:

1. Comply with applicable federal laws that include, but are not limited to, the HHS

Information Security and Privacy Policy (IS2P), Federal Information Security Modernization Act (FISMA), National Institute of Standards and Technology (NIST) Special Publication (SP) 800-series (e.g., 800-53, 800-63), Security and Privacy Controls for Federal 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 HHS, NIH, and NCI Departmental policies.

2. Install software vendor released security patches, update the antivirus definitions to permit automatic updates, and remediate critical and high vulnerabilities in an expedited manner, or within software vendor and agency specified timeframes. Notification of routine updates should occur as part of standard Change Management (see section 5.3.3).
3. Report any potential security breach in accordance with agency-specific incident reporting procedures.
4. Notify the Contracting Officer (CO), Project Manager (PM), and Contracting Officer Representative (COR) within one-hour, upon realization of any potential security breach.
5. Maintain the SAML Single Sign-on (SSO) federated standard to exchange user identity and authentication information between the CORE systems and other information sources for CTEP Clinical Trials (e.g., NCTN group websites).
    a. Expand SSO services for new websites/web-based systems as approved by PM or COR.

5.2.3 System Backup and Disaster Recovery Management

1. Execute the approved Operational Contingency Plan or deviate as needed in the event of any individual system and component failures or failures that need to be addressed prior to execution of the approved Contingency/Disaster Recovery Plan (C/DRP). CTEP-ESYS critical applications shall be operational within 4 hours and be fully operational within 24 hours.
2. Notify the CO, PM, and COR within one-hour, upon realization of any system failure.
3. Work diligently to restore any such failure in the most expedient manner, while providing status updates to the COR as requested by COR post initial synchronous notification until the system failure is resolved.
4. Execute the approved C/DRP or deviate as needed in the event of a disaster causing shutdown of CTEP-ESYS operations (e.g., catastrophic disaster).

5.3 TASK 3 - OPERATIONS AND MAINTENANCE

The work to be performed under this task relates to the operation and maintenance of CTEP-ESYS applications and services. The work may also entail collaboration with a third-party organization to conduct system audit(s) as needed to verify technical and/or functional components.

The Contractor shall:

1. Ensure all CTEP-ESYS applications are fully functional (with the exception of pre-

approved scheduled maintenance), 24 hours per day, 7 days per week.

2. Utilize best practices consistent with Capability Maturity Model Integration (CMMI) maturity level 3 or higher (https://cmmiinstitute.com/learning/appraisals/levels).

3. Comply with information security and privacy requirements, Enterprise Performance Life Cycle (EPLC) processes (see https://www.hhs.gov/sites/default/files/eplc-policy-dec-2016.pdf), HHS Enterprise Architecture requirements to ensure information is appropriately protected from initiation to expiration of the contract. All information systems development or enhancement tasks supported by the Contractor shall follow the HHS EPLC framework.

4. Utilize IT Service Management best practices such as the ITIL framework to help align IT service delivery with business goals.

5. Ensure updates that are compliant with relevant patient consent provisions of Health Insurance Portability and Accountability Act (HIPAA) as applicable to the CTEP-ESYS.

6. Maintain compliance with all regulatory requirements concerning patient records in electronic format that are created, modified, maintained, archived, retrieved, or transmitted under agency record requirements. This compliance also applies to any electronic record submitted to the agency.

7. As appropriate, comply with relevant sections of the Code of Federal Regulations (21 CFR Part 11) for computer systems (including hardware and software).

8. Provide technical and audio-visual support to Government staff for meetings hosted by the Contractor at CTEP facilities and be familiar with the audio-visual systems used at NCI Shady Grove campus after receipt of training from CTEP UC/AV contract located in the facility.

5.3.1 Help Desk

The Contractor shall:

1. Support a CTEP-ESYS help desk supporting CTEP-ESYS end-users, NCI staff and Contractors.

2. Operate the help desk to provide optimal coverage during workdays so CTEP-ESYS end-users across the world will have telephone and email access to help desk staff.

3. Provide after-hours capture of customer support requests (e.g., voice mail, email).

4. Support requests regarding all facets of CTEP-ESYS operations.

5. Provide an initial response to all requests within 4 work hours of receipt during working hours. Requests received during after-hours shall receive a response within 4 hours of the start of the next working day.

6. Develop a triage system to promote rapid and accurate response to queries. Ensure the help desk ticket categorization according to service desk best practices (e.g., ITIL) to differentiate between an incident (e.g., break/fix) or a service request (e.g., see section 5.3.3). All tickets must be categorized and resolved properly to ensure smooth business operations.

7. Work with COR and CTEP Leadership to ensure response timelines are appropriate for the type of assistance requested (e.g., currently CTEP-AERS SAE report submission issues must be addressed within 4 business hours).

8. Develop creative solutions for the help desk functions that enhance relations with CTEP-ESYS clients while simultaneously conserving resources at the help desk to avoid excessive staffing requirements (e.g., FAQs, Quick-tips).

9. Develop mechanisms to track customer satisfaction and identify processes that provide benefit and/or need enhancement.

10. Utilize the help desk log to identify targeted areas to improve CTEP-ESYS operations and user experiences and present those to COR for consideration. This would include repetitive "bugs" or defects that impact day to day work for users.

5.3.2 Incidents (Break/Fix Support)

The Contractor shall:

1. Report any identified defects/bugs found during UAT (including application scan software findings) to the COR prior to release into production. Such defects/bugs should not be put into production unless approved by the COR.

2. Resolve any help desk reported defects/bugs within the time frame required by the COR to ensure the end-user is not impeded from completing their work. If the identified defect(s)/bug(s) cannot be resolved within the timeframe required, devise and implement workarounds with COR approval to overcome system issues and provide resources to adequately handle ad hoc maintenance needs as well as customer support to prevent interruptions until such issues can be addressed.

3. Inform COR within 1 business day of any NIH/NCI noted application scan findings. All findings must be addressed within the timeframe required by NIH/NCI.

5.3.3 Configuration Management (CM)

Information systems that are designed or developed for or on behalf of NIH at non-NIH facilities shall comply with all NIH policies developed in accordance with Federal Information Security Modernization Act (FISMA), NIST, and related NIH security and privacy control requirements for Federal information systems. This includes information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199 system security categorization. The current FIPS 199 categorization is Moderate. The security controls must be designed, developed, approved by NIH, and implemented in accordance with the provisions of NIH security system development life cycle as outlined in NIST Special Publication 800-37.

The Contractor shall:

1. Ensure all CTEP-ESYS system enhancement requests received from stakeholders are vetted through the CTEP CM process to ensure proper evaluation and prioritization of changes to applications in the production environment according to its impact on the customer, implementation complexity, security, and IT resources. The goal of CM is to utilize a structured process to ensure that all system modifications follow an orderly process for evaluation and implementation.

2. Present to the CTEP CM Review Board(s) (CM RB) information necessary to make decisions for authorization and implementation of change requests, depending on the type of change. The CTEP approved Change Request (CR) document shall be used to establish a common understanding and agreement among product owners/stakeholders regarding the scope of changes (data, software, hardware, network, and people). The Contractor lead is responsible for ensuring that the CR document contains supporting information associated with the change request. The Contractor shall use the following guidelines for assessing the change type (see also Table 1):

   a. Standard Change: This change type is a preauthorized change to the service or infrastructure. It has an accepted procedure to deliver a specified change need (e.g., maintenance activities, including but not limited to, updates of codes, reports, XML transactions, patching, system updates). Standard changes must have a written procedure on how they are done. Except in emergency situations, updates and patches must be tested to ensure there is no impact on operations. If the system fails after implementation of updates, the system must be rolled back to its original state, and all findings shall be reported as per the Operational Contingency Plan (see section 5.2.3).

   b. Minor Change: This change type is a modification to the appearance and/or function in one application (e.g., application-specific workflow). The change must not impact the logical data flow of the system, require the hardware to be taken offline, and/or require the software to be restarted without a redundant system to ensure that the software is active for end-users.

   c. Major Change: This change type includes a modification to the appearance and/or function of multiple applications (e.g., end-to-end workflow). This change may involve the addition of new technical components into the data model. Also, it may have an impact on the logical data flow of the system, require the hardware to be taken offline, or require the software to be restarted without a redundant system.

d. Emergency Change: This change type requires the change to be performed quickly to satisfy an immediate need. It may include a repair to an error in a service that is negatively impacting the research mission. An emergency change is a condensed Standard Change and, if possible, the change must be tested before implementation. Immediate notification to the COR is required upon realization of any system failure for any reason.

Table 1: Change Type(s)

Category	Standard	Minor	Major	Emergency
Risk Impact	Low	Low-Moderate	High	Unknown
Application(s)	One or many	One	Many	Unknown
Content	Accepted procedure	Display and format (Layout)	Logical/Physical Data flow	Unknown
Contracts	One or many	One	One or many	One or many
Reason	Routine updates	End-user request	End-user request	Satisfy an immediate need
Operations	No Impact	No impact (End-user training)	May Impact (End-user training)	Unknown

3. Work with end-users and other NCI Contractors to document the business process flow/s, gather requirement/s, and classify the change/s. The Contractor shall review the current state with every change request to ensure standardization of system workflows and content. The Contractor shall consider ways to reduce complexity of maintenance tasks, support data quality and increase ease of use of the application and other integrated systems.

4. Work with end-users and other NCI Contractors to validate the business specifications to ensure the change is aligned with operational, regulatory, and scientific needs (e.g., conform with terminology standards for data exchange and FDA reporting, support research data collection in cancer Data Standards Repository (caDSR), support existing or new trials, aligned with operational requirements of NIH/NCI and new/current MCOs).

5. Ensure that the CR document includes detailed requirements with clear assignment to a specific component within the system and associated challenges/risks. The CR document

shall include corresponding documentation (e.g., Implementation Plan, Training Plan) and shall contain targeted performance improvement goals.

6. Ensure conformity to the CM process. Change requests must be presented to the CM RB for discussion unless otherwise directed by the COR. The phases of scheduling, building, testing, and implementation may commence upon receiving approval via email from the COR.

7. Ensure that any CM RB(s) recommendations and the final COR decision are entered in the CR document and the COR decision is communicated back to the requestor.

8. After the change is complete, the Contractor shall document the status (e.g., implemented, failed, or backed out) and lessons learned in the CR document. All new and closed CR documents shall be uploaded in the COR designated storage location with the appropriate naming convention approved by the COR. Status update should be provided during change review meeting(s).

9. Collaborate with other NCI Contractors on enhancement and integration activities to ensure that the functional and technical specifications meet the customer's needs, and work with internal and external stakeholders to identify system improvements to eliminate waste (e.g., retire redundant features/systems) and decrease resources for system maintenance and support.

10. Collaborate with other NCI Contractors on access management activities to prevent permission creep, e.g., analyze system workflows to ensure that system profiles, roles, and permissions are designed to match the user's function within the organization.

5.3.4 System Manuals and Training

The Contractor shall:

1. Maintain a set of up-to-date Administrator/System manuals detailing the operational procedures and business rules for all CTEP-ESYS applications. These manuals should be reviewed and approved by the COR prior to posting. The updated set of manuals should be posted online to a secure reading room. Administrator/System manuals should be updated as needed with revised versions posted for review and use by project leadership team.

2. Maintain a set of up-to-date user guides for all CTEP-ESYS applications. User Guides should be maintained on the appropriate applications landing page after log in. These user guides should be reviewed and approved by the COR or designee prior to posting. User guides should be updated as needed and/or as requested by the COR.

3. Develop, update, maintain, and provide training and education materials for all applications (e.g., integrations, enhancements) and provide training to Government and other stakeholder personnel at the direction of the COR. Upon request by the COR,

education and training materials must be provided in a format compatible with the CLASS Learning Management System.

4. Develop and support enhanced communication regarding CTEP-ESYS activities with stakeholders through the use of, but not limited to, monthly project review meetings, release notes, trainings sessions, and presentations.

5.3.5 IT Planning, Reports and Data Calls

The Contractor shall:

1. Submit data as requested by HHS, NIH, and/or the Office of Management and Budget (OMB) to respond to data calls; populate Major Investment business cases and maintain an acceptable rating. The Contractor shall manage the update and upload process for monthly submissions as well as ad hoc data calls. All submissions shall be reviewed and approved by the COR prior to submitting to FOLIO (or other reporting tool in use by NIH or HHS at that time) or in response to a data call.

2. Provide any scheduled reports and conduct queries of CTEP-ESYS data as needed. To protect patient confidentiality and proprietary data all requests shall first be reviewed and approved as required per the CTEP SOP. The COR shall be copied on all such correspondence.

3. Comply with all requirements stated in the Reporting Requirements/Deliverables Section of the Task Order as well as the requirements pertaining to HHS IT Security Section.

4. Work with all relevant and affected stakeholders, including CTEP personnel and Contractors as well as grantees and other clinical trial site staff to help achieve the NCI's mission. This may include but is not limited to, training sessions, requirements gathering sessions, beta testing, etc.

5.4 TASK 4 – INFORMATION MANAGEMENT

The work to be performed under this task relates to collection, management, storage, sharing, and delivery of CTEP data.

5.4.1 Data Repositories/Warehouse

The Contractor shall:

1. Maintain and enhance existing CTEP-ESYS data repositories, including but not limited to the CTEP CORE Central Data Repository (CDR).

2. Identify vulnerabilities that may impact system performance, data integrity, and security and recommend alternatives to mitigate the risks and implement the solution(s) to resolve the risks upon approval from CTEP leadership.

3. Utilize Extract-Transform-Load (ETL) tools and implement best practices to ensure data quality upon transfer.

4. Proactively work with CTEP leadership and system leads, as directed by COR to develop best practices, generate data strategies, build data flows, and develop conceptual/logical/physical enterprise data models.

5. Establish and/or maintain privilege and role authorization controls to assign/revoke permissions to access, process or modify CTEP data. Implement appropriate multi-factor authentication (MFA) procedures to verify users.

5.4.2 System Integrity and Interoperability

The Contractor shall:

1. Collaborate with other NCI Contractors and grantees to enhance and/or expand CTEP-ESYS integration with other systems within and/or outside the NIH perimeter firewalls to include, but not limited to:

   a. NCI systems: The CTEP-ESYS shall interface and allow 2-way sharing of selected information, as needed, with other NCI-owned systems including, but not limited to, CTSU-Enterprise System (CTSU-ESYS), DCP's Protocol Information Office Clinical Trials System (PIO-CTS), Medidata Rave, Clinical Trials Reporting Program (CTRP), and the Central Institutional Review Board (CIRB) application suite.

   b. Other systems: e.g., Clinicaltrials.gov; LPO clinical trial applications

2. Share information, business processes, data models, training materials, and any additional artifacts (at the direction of the COR) to promote efficiency and effectiveness, reduce administrative burden, and ensure collaboration with members of the NCI and oncology community.

3. Utilize relevant syntax (e.g., API) and semantic (e.g., terminology/code) standards to support proper communication, interpretation, and computability of transmitted data elements.

4. Seek ways to enhance system interoperability and improve data integrity in support of the research mission. For example, the Contractor shall ensure that standardized terminologies (e.g., Logical Observation Identifiers Names and Codes (LOINC), Clinical Data Interchange Standards Consortium (CDISC), NCI terms, NLM terms) are implemented to promote data interoperability as per medical research standards.

5. Maintain compliance with all regulatory requirements concerning patient records in electronic format that are created, modified, maintained, archived, retrieved, or

transmitted under agency record requirements. This compliance also applies to any electronic record submitted to the agency as well as the format and standards in which they are transmitted (e.g., CDISC, XML, E2B, etc.). Conform to industry best practices such as CDISC and Health Level 7 (HL7) standards for electronic data transfer. http://hl7.org/fhir/terminologies-systems.html

6. Update/Incorporate CDISC standards into current and future CTEP-ESYS applications and services accessed by:

   a. External entities and systems that either partially map or don't map with required variables (e.g., CDASH/SDTM).

   b. Internal entities and systems (e.g., other NCI or CTEP Clinical Oncology Research Enterprise [CORE] systems/entities) that either partially map or don't map with required variables (e.g., CDASH/SDTM).

7. Provide technical and subject matter expertise support to assure effective utilization of common data elements (CDEs) to enhance semantic interoperability.

8. Interface with the enterprise vocabulary system (EVS) developed by the NCI. https://evs.nci.nih.gov/

5.4.3 508 Compliance Requirements

This requirement is considered an Information and Communication Technology (ICT) product or service. The Contractor will be required to develop, procure, maintain, and/or use ICT and to ensure their EIT allows Federal employees and members of the public with disabilities to have access to, and use of, information and data comparable to the access and use by people without disabilities. The following 508 standards shall be employed: Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use information and communication technology (ICT), it shall be accessible to people with disabilities. Federal employees and members of the public who have disabilities must have access to, and use of, information and data that is comparable to people without disabilities.

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

2. Per Section 508 and as mandated under HHS Policy for Section 508 Compliance and Accessibility of Information and Communications Technology (ICT) (07/2020) all documents or electronic files provided to the NIH NCI under contract must be conformant with Section 508 standards and accessible to persons with disabilities. Conformance shall be confirmed by use of material provided at HHS OS

Factsheets & Reference Guides and verified through the use of the HHS Checklist Documents (WCAG 2.0 Refresh); in addition, Contractors and vendors are encouraged to make use of the instructional materials and checklists at GSA Section 508.gov's Create Accessible Digital Products.

Items in this parent contract or Statement of Work that contains ICT:

- Call (Contact/Help Desk) Center Services
- Cloud Computing
- Computer-based Training
- Data Services or Information Retrieval Systems
- Electronic Documents
- Information Content Services
- Internet and Intranet websites and web-based content
- Internet or Intranet Services
- Management Information System Services
- Software
- Software Development Services
- Software Maintenance Services
- Web Application
- Web Application Maintenance
- Web-based Collaboration Tools
- Web-based Information, Documentation and Support
- Web-based Training

Further guidance can be found at https://section508.gov/, including its Standards Applicability Checklist for any other ICT deliverables as part of this acquisition. Resources, addition to the following, will be provided or made available, to the Contractor:

- Department of Health & Human Services' (HHS) Accessibility Compliance Checklists
- GSA's Section508.gov and its section on Create Accessible Digital Products

The Accessibility Conformance Report (ACR) should be based on/developed from the Voluntary Product Accessibility Template® (VPAT®), Revised Section 508 Edition, Version 2.4 (VPAT 2.4Rev 508 (February 2020) (March 07, 2020))

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

Applicable requirements for software features and components: All WCAG Level AA Success Criteria, 502 Interoperability with Assistive Technology, 503 Application

Applicable requirements for hardware features and components: All requirements apply.

Applicable support services and documentation: All requirements apply.

6. TRANSITION ACTIVITIES

The Phase-In coincides with the start of the contract period and is not a separate Option. The Phase-In shall be for a period of up to three months. The Contractor shall assist in the transition from a predecessor Contractor (Phase-In), and of this contract to a successor Contractor (Phase-Out), when applicable. A Phase-Out transition period shall consist of 3 months after the expiration date of the contract.

6.1 Phase-In Transition

Within seven (7) calendar days of the award, the draft Phase-In Transition Plan submitted with the proposal shall be revised, if necessary, and shall become the final Phase-In Transition Plan upon approval of the Contracting Officer's Representative (COR). Upon approval of the Contractor's Phase-In plan, the Contractor shall meet with the predecessor Contractor for briefings on execution of the Phase-In plan. The Contractor shall work with the predecessor Contractor to ensure that work operations are fully understood, and continuity of operations are maintained through the transition. The final Phase-In Transition Plan shall be followed to ensure an orderly, secure, efficient, and expedient transition of all contract activities.

6.2 Phase-Out Transition

The Contractor shall prepare and submit a draft Phase-Out transition plan to facilitate the accomplishment of a seamless transition. The draft plan will describe the Contractor's strategy for transferring their knowledge of the work from this contract to a successor contract, in the event a final transition would be required. In accordance with the delivery schedule, the draft Phase-Out Transition plan shall be submitted to the COR and Contracting Officer no later than six (6) months prior to the expiration of the TO. The draft plan must include a system for transfer of policies and procedures; transfer of relevant files, records, materials and data; all source code and object code developed, modified and/or enhanced under the contract; transition of all activities, and transition of all CTEP-ESYS applications, as appropriate. The draft plan will be revised as needed and shall become the Final Phase-Out Plan upon approval of the COR.

The Contractor will execute the transition out activities In Accordance With (IAW) the Government-approved Phase-Out Transition Plan to ensure an orderly, secure, efficient, and expedient transition of all contract activities.

OPTIONAL TASKS

1. Option A for Hardware Sustainment and Backed-Up Data Storage

The Contractor shall be required to maintain the CTEP infrastructure at the NIH or NCI data center following all the data center requirements.

a. Equipment

The Contractor shall:

1. Provide and maintain all equipment that is necessary for CTEP-ESYS environment or service that is not provided by data center. It is expected that hardware refresh by the Contractor should take place at a minimum every 5 years from date of purchase or as required for hardware that has reached End of Service/Support Life (EOSL) or where newer software/operating systems that will not operate on an older server. All hardware purchases must meet NIST standards (e.g., may not purchase or supply servers from companies listed on the Federal No Buy List).
2. Manage all CTEP-ESYS related equipment including shut down and restarts.
3. Maintain documentation of the inventory in a manner approved by the COR.
4. Be responsible for capacity planning to ensure that the equipment is adequate to maintain the high availability of the systems deemed vital to CTEP operations.

b. Security

The Contractor shall:

1. Ensure that proper security protocols are enabled for all of the equipment and systems in the data center.
2. Ensure security agents are operating and current on all servers.

c. Monitoring

The Contractor shall:

1. Monitor all CTEP-ESYS provided equipment.

d. Facility Safety

The Contractor shall:

1. Shut down any CTEP-ESYS provided equipment if the Contractor detects that it presents a hazard, is doing harm to, or has harmed the facility.
2. Adhere to rules of behavior specified in the NCI Data Center Policy and Work Rules document.

The Contractor shall work with the COR as directed to seek opportunities to improve the operational effectiveness of the data center environment (e.g., other hosting models) and recommend alternatives to safeguard the CTEP IT infrastructure, increase system performance, and/or increase cost savings.

In addition to SOW Task 2: System Back Up, the Contractor shall:

1. Provide backed-up data storage with capacity to hold up to one year of data in a secure location no less than 25 miles physically away from the primary data center (e.g., tapes at a secure remote facility, CLOUD).
2. Ensure backed-up data stored at these location(s) is available in such a fashion as to ensure rapid recovery of CTEP-ESYS services to meet the SLA requirements.

2. Option B for Primary Data Center Migration Services

Data Center Migration Services are the Services and Activities, as further detailed below required to migrate Servers and Operating Systems (both physical and virtual environments), Storage Hardware, Tape Libraries, and IP Console Switches from their current NIH data center location to a new data center location (e.g., NCI)

The Contractor shall be responsible for the identifying, prioritizing, provisioning in the new environment, performing a safe and secure migration, testing and certifying of all applications and related equipment from the current data center to the new environment. In addition, the existing data centers may have additional requirements that need to be met per the current hosting model requirements. The Contractor shall be responsible for each Phase of this migration.

Phase I – Application, Data Architecture Discovery and Mapping

This phase shall include surveying and documenting the existing data center architecture. During the Application and Data Architecture phase the Contractor shall identify and document current services, map services to equipment and prioritize migration and availability based on business needs, helping to mitigate migration risks and identify tools and technologies that expedite recovery. This phase shall include:

- Application identification and prioritization for recovery and migration
- Application dependency mapping for inbound and outbound data
- Application to server mapping and server prioritization
- Forecasting future growth and capacity planning of applications, data, and infrastructure
- Discovery and inventory of application-specific network connections to be migrated
- Application virtualization opportunity identification and prioritization
- Application availability analysis and migration window options
- Backup and disaster recovery identification and migration planning

Phase II – Migration Plan

This phase shall include planning the physical move of equipment, and virtual migration of applications / data from the existing data centers into the new data centers. Migration shall be performed with zero downtime for IAM and all application modules within CTEP-ESYS during CTEP peak working hours. The Contractor shall coordinate and ensure connectivity and communication with other CTEP-CORE Contractors and that it is available during CTEP peak business hours.

The Contractor shall design a systematic process that encompasses planning and coordination with the new co-hosted data center staff including:

- Identification of migration options for servers and applications including rack optimization, power requirements and “forklift” vs. over-the-wire migration options
- Identification of any services and equipment needed.
- Development of communication plan for different levels of management/Contractors
- Floor space design for placement of equipment and racks
- Application virtualization planning, with sequence and testing scenarios
- Identification of migration risks and mitigating actions associated with migrating

application and servers
- Identification of any security issues that will need to be addresses as well as any data protection, temporary or replacement accounts that will be needed and actions to be taken
- Development of data center physical migration project plan and Work Breakdown Structure (WBS) in an industry standard project planning tool and maintaining it in a CTEP approved tool
- Design of migration program management responsibilities
- Network (WAN and LAN) preparation and certification for migration
- Identification of all equipment/fixtures/infrastructure to be removed after migration (if any)
- Identification of options for cost, disposal (including cost recovery) and/or reuse of equipment
- Identification of services to be decommissioned, with any associated lead times and costs for discontinuation of services

Contractor shall coordinate with the new co-hosted data center team as they may be able to provide a pre-migration checklist.

Phase III – Data Center Migration
The Contractor shall manage and monitor the physical move of servers along with all associated system components, migration of all applications and associated data including, but not limited to:

- Implementation of plans and preparation completed in Phase II
- Coordination and preparation of facility for migration
- The new data center readiness preparation and certification for migration
- New equipment installation
- Server and other equipment migration
- Security assurance of physical and logical assets
- Inventory control
- Application and data migration, including migration to virtual environment
- Complete data center service availability, testing, and certification

Note: During all stages of migration, FISMA compliance must be maintained and assured. The Contractor must coordinate with various internal and external stakeholder teams involved with NIHNET and dependent services.

Phase IV – Post-Implementation Services
During this phase, the Contractor will dispose of or salvage any remaining equipment in the old data centers that is not a part of the original data center facility or otherwise contractually required to be removed from the facility. This phase, includes, but is not limited to:

- Revalidation of post implementation plans including pre and post diagrams, decommission lists, and dispositions
- Identification of all equipment to be removed from the premises
- Identification of options for cost: disposal (including cost recovery) and/or reuse of equipment

- Identification of services to be decommissioned, with any associated lead times and costs for discontinuation of services
- Ensure that removal of any data storage devices is done after complete destruction of data.
- Ensure that all temporary accounts, any unused or migrated accounts and any other security related items are closed out in accordance with NIH and NCI security policies.

3. **Option C for Secondary Data Center Migration Services**

Data Center Migration Services are the Services and Activities, as further detailed below required to migrate Servers and Operating Systems (both physical and virtual environments), Storage Hardware, Tape Libraries, and IP Console Switches from their current NIH (Sterling, VA) data center location to a new data center location (e.g., NCI)

The Contractor shall be responsible for the identifying, prioritizing, provisioning in the new environment, performing a safe and secure migration, testing and certifying of all applications and related equipment from the current data center to the new environment. In addition, the existing data centers may have additional requirements that need to be met per the current hosting model requirements. The Contractor shall be responsible for each Phase of this migration (same requirements as Option B)

Appendix 1 – CTEP Resources

- CTEP Website Homepage: https://ctep.cancer.gov/
- CTEP Mission: https://ctep.cancer.gov/about/default.htm
- CTEP Organizational Chart: https://ctep.cancer.gov/about/org_chart.htm

Appendix 2 – Acronym Glossary

A&A – Assessment and Authorization process
ABTC – Adult Brain Tumor Consortium
ACOSOG - American College of Surgeons Oncology Group
ACRIN – American College of Radiology Imaging Network
AdEERS – Adverse Event Expedited Reporting System
AET – Awareness Education and Training
ASCO – American Society of Clinical Oncology
ASM – Application Support and Maintenance
AYA –Adolescents and Young Adult
BMT-CTN – Bone Marrow Transplant Clinical Trials Network
BRP – Biometric Research Program
BRIDG – Biomedical Research Integrated Domain Group
caAERS – cancer Adverse Event Reporting System
caDSR – Cancer Data Standards Repository
CBIIT – Center for Biomedical Informatics and Information Technology
CCCT – Coordinating Center for Clinical Trials, NCI
CCOP – Community Clinical Oncology Program
CCP – Cancer Centers Program
CDE – Common Data Elements
CDISC – Clinical Data Interchange Standards Consortium
CDMS – Clinical Data Management System
CDUS – Clinical Data Update System
CEP – Concept Evaluation Panel
CEWS – CTSU Enterprise Web Services
CFR – Code of Federal Regulations
CGCB – Clinical Grants and Contracts Branch
CIB – Clinical Investigations Branch
CIP – Cancer Imaging Program
CIRB – Central Institutional Review Board
CIT – Center for Information Technology
CITN – Cancer Immuno-Therapy Network
CMMI – Capability Maturity Model Integration
COBIT– Control Objectives for Information and Related Technology
COG – Children's Oncology Group
CO – Contracting Officer
COR – Contracting Officer’s Representative
COTS – Commercial off-the-shelf product
CPIC – Capital Planning and Investment Control
CRADA – Clinical Research and Development Agreement
CRF– Case Report Form
CSC – CDMS Support Center
CTA – Clinical Trials Agreement
CTCAE – Common Terminology Criteria for Adverse Events
CTEP – Cancer Therapy Evaluation Program

CTEP IAM – CTEP Identity and Access Management
CTEP-AERS – CTEP Adverse Event Reporting System
CTEP-ESYS – Cancer Therapy Evaluation Program – Enterprise System
CTMB – Clinical Trials Monitoring Branch
CTMB-AIS – CTMB Audit Information System
CTRP – Clinical Trials Reporting Program
CTSU – Clinical Trials Support Unit
CTSU-ESYS – CTSU Enterprise System
DARTS – Drug Authorization, Review and Tracking System
DBMS – Database Management System
DCP – Division of Cancer Prevention
DCS – Developmental Chemotherapy Section
DCTD – Division of Cancer Treatment and Diagnosis,
DHHS – Department of Health and Human Services
DMAS – Drug Management and Authorization Section
DTP – Developmental Therapeutics Program
ECM – Enterprise Core Module
ECOG – Eastern Cooperative Oncology Group
eCRF – electronic Case Report Form
EIT– Electronic and Information Technology
EPLC – Enterprise Performance Life Cycle
ETCTN – Experimental Therapeutics Clinical Trials Network
EVM – Earned Value Management
EVS – Enterprise Vocabulary System
FDA – Food and Drug Administration
FIATS – Funding Instrument & Accrual Tracking System
FISMA – Federal Information Security Management Act
HIPPA– Health Insurance Portability and Accountability Act
HL7 – Health Level Seven
HSPD-12 – Homeland Security Presidential Directive-12
ICT – Information and Communication Technology
IDB - Investigational Drug Branch
IDSC – Investigational Drug Steering Committee IT
IND – Investigational New Drug Application
IPAD – Integrated Platform for Agents and Diseases
ITIL – IT Infrastructure Library
LAN – Local Area Network
LOI – Letter of Intent
LOINC – Logical Observation Identifiers Names and Codes
NCI – National Cancer Institute
NCIP – National Cancer Informatics Program
NCORP – NCI Community Oncology Research Program Community
NCTN – NCI National Clinical Trials Network
NIH – National Institutes of Health
NIH AD – NIH Active Directory
NIST – National Institute of Standards and Technology

OMB – Office of Management and Budget

OPEN – Oncology Patient Enrollment Network

PDQ – The Physician Data Query

PIO – Protocol and Information Office

PM – Project Manager

PMB – Pharmaceutical Management Branch

PRS – Performance Requirements Summary

QA – Quality Assurance

RAB – Regulatory Affairs Branch

RABITS – Regulatory Affairs Branch Information Tracking System

RDBMS – Relational Data Base Management System

ROI – Return on Investment

RRP – Radiation Research Program

RUP – Rational Unified Process

SOA – Service-oriented architecture

SSO – Single Sign On

START System - Study Abstraction Review & Tracking System

TQM – Total Quality Management

TQS – Total Quality Systems

XML – Extensible Markup Language

Appendix 3 – CTEP-ESYS Applications and CTEP CORE Centralized Data Repository

AdEERS Backend System (ABS)

- Production: 2001
- Users: IDB support Contractor, CTOIB
- Functionality:
    - Review and assessment of the Adverse Events (AEs)

AURORA

- Production: 2018
- Users: PMB Pharmacists, Clinical Repository Users, Clinical Trial Sites Designees
- Functionality:
    - Manage clinical inventory (inventory, orders, transfers, returns)
    - Mange Electronic Drug Accountability (eDARFs)
    - Acquisitions and Receipts/ Labels creation including Receipt Reports
    - Manage drug ordering and shipping (In Progress/ To be completed)

Centralized Data Repository (CDR)

- Production: 2017
- Users: CTEP, CTEP Contractors
- Functionality:
    - Consolidate data from multiple data providers
    - Harmonize information across disparate systems

CTEP Adverse Event Reporting System (CTEP-AERS)

- Production: 2013
- Users: CTOIB, IDB support Contractor, Groups, Consortia, Networks, and other Institutions that participate in NCI- sponsored trials
- Functionality:
    - Create and manage protocol-specific Adverse Event reporting rules
    - Provide recommendations whether an expedited reporting of Adverse event is recommended
    - Capture Adverse Event information
    - Facilitate submission to NCI and/or predetermined recipients
    - Submission reminder notifications

Clinical Data Update System (CDUS)

- Production: 1998
- Users: Groups, Consortia, Networks, and other Institutions that participate in NCI-sponsored trials, CDUS Operations Team
- Functionality:
    - Load protocol data on patients enrolled on NCI sponsored trials
    - Smart Loader: validates data files and sends results to submitters
    - Correspondence: Sends initial codes and follow-up emails to submitters
    - Reports: Standard output format for reviewing data

Clinical Investigations Branch Information System and Clinical IT (CIBISCIT)

- Production: 2005
- Users: Protocol Abstraction- CIB support Contractor, Accomplishments-CIB
- Functionality:
    - Assist the Clinical Investigations Branch (CIB) (i.e., data entry, storage, reporting, analysis, retrieval) of information related to diseases to be studied in Concepts and Phase III protocols
    - Detailed Protocol Abstraction
    - Accomplishment management
    - Disease Profile Reports

Clinical Trials Monitoring Branch- Audit Information Systems (CTMB-AIS)

- Production: 1999
- Users: CTMB, NCTN, NCORP Research Bases, AMC, PBTC, CTMS
- Functionality:
    - Schedule Audits and CTMS visits
    - Generate audit/monitoring visit reports
    - Review Audit results and monitoring reports and uploaded CAPA plans/responses
    - Manage network group rosters
    - View CTMS Phase 1/Phase 2 roster, PEP-CTN rosters

Comprehensive Adverse Event and Potential Risk System (CAEPRS)

- Production: 2007
- Users: CTEP support Contractor staff and IDB
- Functionality:
    - Maintain the risks and adverse events lists for agents

CTEP Enterprise Services (CES)

- Production: 2008
- Users: External: CTRP, DCP, CTSU
- Functionality:
    - Study Details and LOV services provide data elements related to protocols
    - Organization Service provides data elements related to organizations
    - Person Service provides data elements related to persons
    - Roster Query Service and Validation Service for institutions
    - Adverse Events Services

Dose Regimen (Dose Reg)

- Production: 2000
- Users: PMB
- Functionality:
    - Summary description based on detailed dosing regimen entry

Drug Authorization, Review and Tracking System (DARTS)

- Production: 1999

- Users: PMB, Agent Repository staff
- Functionality:
  - Manage clinical inventory (inventory, orders, transfers, returns)
  - Manage blinded protocols (integrated order entry with collaborators)
  - Manage treatment referral center data

Enterprise Core Module (ECM)

- Production: 2004
- Users: Request/Query-CTEP Staff, Review/Approval-PMB Coordinators
- Functionality:
  - Query Organizations, persons
  - Request new organization, request new person
  - Review/Approve requests

Enterprise Maintenance System (EMS)

- Production: 1998
- Users: Select CTEP staff and Contractors
- Functionality:
  - Maintain agents, disease specialists, protocol specialists, POP Track

Funding Instrument and Accrual Tracking System (FIATS)

- Production: 1999
- Users: CTEP Grants managers and Contractor staff
- Functionality:
  - Capture grant related data
  - Manage the funding aspects of the Phase II contracts and other grants supporting NCI-sponsored clinical trials for IND agents

Identity and Access Management (IAM)/Single Sign On (SSO)

- Production: 2007
- Users: CTEP and DCP staff and Contractors as well as all study personnel involved in the conduct of NCI-sponsored clinical trials
- Functionality:
  - Manage user accounts (request, approval, re-registration, access control)
  - Provide secure login, authenticate user account (web)
  - SAML 2.0 implementation provides Single Sign On capability and federated authentication

Integrated Platform for Agents and Diseases (IPAD)

- Production: 2010
- Users: CTEP, DCP and select NCI staff and support Contractors
- Functionality:
  - Enterprise search/Query data related to LOIs, protocols, and concepts, Agents, AEs, Accrual data

Online Agent Order Processing (OAOP)

- Production: 2010
- Users: PMB professional and extramural support staff (i.e., Authorizers, Investigators, and Repository)
- Functionality:
    - Manage agent order processing online for Investigator (ordering designee), Authorizer and Repository

Registration and Credentialing Repository (RCR)

- Production: 2017
- Users: PMB Pharmacists, Investigators, Registration Coordinators, Designees and Clinical Site Users
- Functionality:
    - Provides a self-service online person registration application with electronic signature and submission capability

Regulatory Affairs Branch Information Tracking System (RABITS)

- Production: 2005
- Users: RAB users
- Functionality:
    - Manage research agreements such as Clinical Trials Agreements (CTAs) and Cooperative Research and Development Agreements (CRADAs)
    - Preparation and submission of INDs and associated IND amendments
    - IND Details Management

Safety Profiler (CTCAE) Tool

- Production: 1999
- Users: Data managers, nurses, clinical research assistants and PIs at cancer cooperative groups (Groups), consortia, networks, and single institutions
- Functionality:
    - View and search through multiple versions of CTCAE
    - Search by category, keyword, or literal text across all CTCAE versions

Scientific Management of Agents Review and Tracking System-Annual Reports (AR)

- Production: 2000
- Users: IDB support Contractors
- Functionality:
    - Generate Biologic/Chemotherapeutic Annual Report
    - Query and Save Annual Report for a specific IND

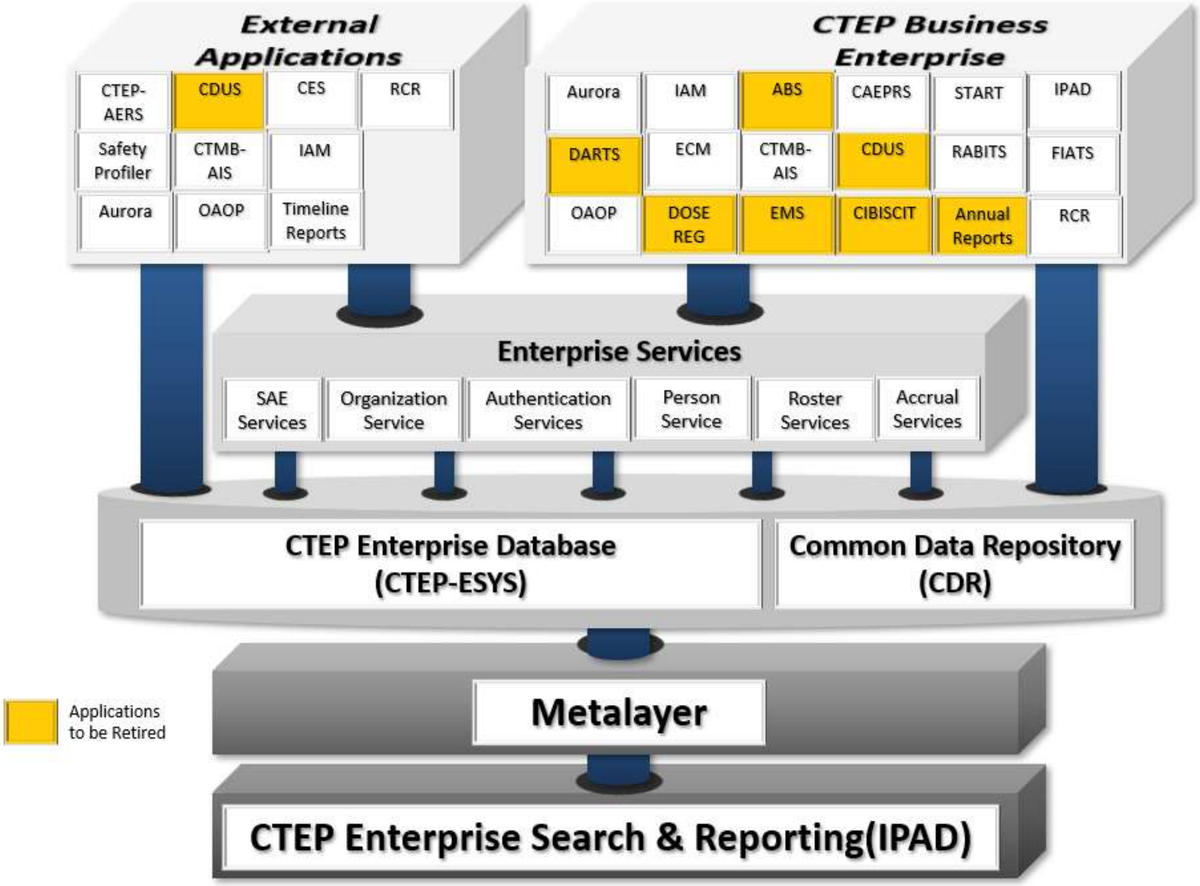
Secure Website (Timeline Reports)

- Production: 2010
- Users: CTEP staff and support Contractors, Groups, Consortia, Networks, and other Institutions that participate in NCI- sponsored trials
- Functionality:

  - Organization and Document Search
  - Protocol Development Timeline (PDT) reports

Study Abstraction Review & Tracking System (START)

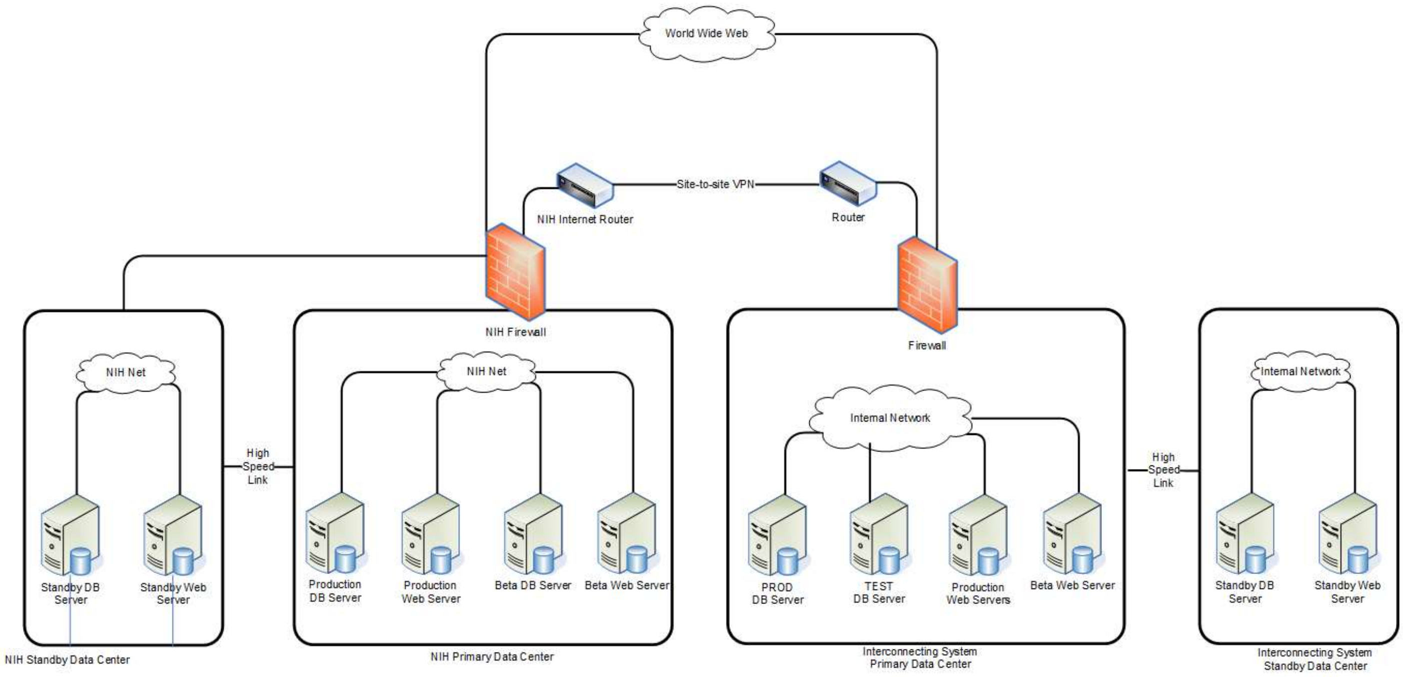
- Production: 2017
- Users: CTEP, CTEP Contractors, DCP, CIP, CDP and other support Contractors
- Functionality:
  - Abstract high-level study details
  - Tracking Study Development Milestones
  - Biomarker abstractions and Milestones
  - Generate study correspondence/ letters
  - Search and Reporting capabilities to support user needs
  - Document, storage Search and Reporting capabilities



CTEP-ESYS Schematic Diagram (Current)

Appendix 4 – CTEP-ESYS Interconnections

CTEP-ESYS Connectivity with Interconnecting Systems (current)


World Wide Web
NIH Internet Router
Site-to-site VPN
Router
NIH Firewall
Firewall
NIH Net
Standby DB Server
Standby Web Server
NIH Standby Data Center
High Speed Link
NIH Net
Production DB Server
Production Web Server
Beta DB Server
Beta Web Server
NIH Primary Data Center
Internal Network
PROD DB Server
TEST DB Server
Production Web Servers
Beta Web Server
Interconnecting System Primary Data Center
High Speed Link
Internal Network
Standby DB Server
Standby Web Server
Interconnecting System Standby Data Center