Attachment 5

06.1 HHS Privacy Impact Assessment (Form) / NIH NCI Cancer Trials Support Unit (CTSU (Item)
Form Report, printed by: Mehta, Jay, Feb 4, 2009

PIA SUMMARY

1

The following required questions with an asterisk (*) represent the information necessary to complete the PIA Summary for transmission to the Office of Management and Budget (OMB) and public posting in accordance with OMB Memorandum (M) 03-22.
Note: If a question or its response is not applicable, please answer "N/A" to that question where possible. If no personally identifiable information (PII) is contained in the system, please answer questions in the PIA Summary Tab and then promote the PIA to the Senior Official for Privacy who will authorize the PIA. If this system contains PII, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

2 Summary of PIA Required Questions

*Is this a new PIA?:	Yes
If this is an existing PIA, please provide a reason for revision:	
*1. Date of this Submission:	Feb 27, 2009
*2. OPDIV Name:	NIH
*3. Unique Project Identifier (UPI) Number for current fiscal year:	TBD
*4. Privacy Act System of Records Notice (SORN) Number (If response to Q.21 is Yes, a SORN number is required for Q.4):	09-25-0200
*5. OMB Information Collection Approval	TBD

Number: *6. Other Identifying Number(s):	TBD
*7. System Name (Align with system item name):	NIH NCI Cancer Trials Support Unit (CTSU)
*9. System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:	

Point of Contact Information

POC Name Mike Montello

*10. Provide an overview of the system:	The Cancer Trials Support Unit (CTSU) is a service offered by the National Cancer Institute to enhance and facilitate access to cancer clinical trials for clinical investigators in the United States and Canada. The CTSU maintains a broad menu of trials developed by the adult cancer Cooperative Groups and other research consortia and works with these organizations to offer patient enrollment, data collection, data quality management, and enrollment reimbursement services to clinical sites entering patients in these trials. In addition, the CTSU offers a regulatory support service to all adult cancer clinical trials by collection of regulatory documents and maintenance of a national database of investigators and sites. The CTSU also provides education and training for clinical site staff and clinical trials promotion services to help increase enrollment in cancer trials. A large and complex information technology infrastructure has been developed to support CTSU operations and exchange data with other data centers involved in cancer research. Westat is the prime contractor on the project, having two subcontractors, and working with numerous other organizations.
*13. Indicate if the system is new or an existing one being modified:	Existing
*17. Does/Will the system collect, maintain (store),	Yes

disseminate and/or pass through PII within any database(s), record(s), file(s) or website(s) hosted by this system?: Note: This question seeks to identify any, and all, personal information associated with the system. This includes any PII, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation.	
*21. Is the system subject to the Privacy Act? (If response to Q.19 is Yes, response to Q.21 must be Yes and a SORN number is required for Q.4):	Yes
*23. If the system shares or discloses PII, please specify with whom and for what purpose(s):	CTSU shares NCI Investigator and NCI Associates data with CTEP-ESYS – a NCI sponsored project and other Cooperative Groups, to increase participation in NCI sponsored cancer related clinical trials. With increased awareness and access to the trials information, CTEP intends to increase physician and patient participation in the NCI sponsored trials. CTSU shares this information, which may contain IIF, with lead research

	organizations for the purpose of assuring patient safety, for scientific decision making, drug distribution, regulatory oversight (i.e., investigator registration; trial audits) and to facilitate administrative operations. CTSU also shares this information with the Cooperative Groups and with NCI Center for Biomedical Informatics and Information Technology's Clinical Data System (CBIIT-CDS). Some of this information is available to staff at Cooperative Group member sites on a limited basis. Some of the information that CTSU shares with CTEP and CBIIT-CDS is also publicly available elsewhere.
*30. Please describe in detail: (1) the information the agency will collect, maintain, or disseminate; (2) why and for what purpose the agency will use the information; (3) in this description, explicitly indicate whether the information contains PII; and (4) whether submission of personal information is voluntary or mandatory:	Legislation authority is the Public Health Service Act (42 U.S.C. 241, 242, 248, 282, 284, 285a-j, 285l-q, 287, 287b, 287c, 289a, 289c, and 44 U.S.C. 3101.). The types of data used are scientific and health data about cancer clinical trials, including clinical and pre-clinical data with associated regulatory and administrative supporting information. Patient participation in CTEP clinical trials is voluntary and participants in CTEP clinical trials sign an informed consent. Types of information available in the CTSU Enterprise include protocols and protocol attributes, Investigator registration details, and non-IIF patient accrual details. The information is used to assure patient safety, for scientific decision making, drug distribution, regulatory oversight (i.e., investigator registration; trial audits) and to facilitate administrative operations. The CTSU collects and maintains various types of data. Investigator and treatment site staff information is obtained from the CTEP-ESYS and maintained in the CTSU. Cooperative Group staff use this data to maintain their membership rosters. This data is used as part of the credentialing requirements for patient enrollments. Protocol and regulatory information related to the member sites is collected and maintained in the CTSU Enterprise. This data is disseminated to Cooperative Groups to support patient enrollment and data collection processes. The CTSU also performs patient enrollments and will begin to collect demographic, eligibility criteria data, and other enrollment required data as part of this process. This data is collected on behalf of and shared with the organization that is leading a study. For some studies, the CTSU performs the complete data management

	and collects/maintains the clinical data collected for a study and disseminates it to the organization leading the study.
*31. Please describe in detail any processes in place to: (1) notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of the original collection); (2) notify and obtain consent from individuals regarding what PII is being collected from them; and (3) how the information will be used or shared. (Note: Please describe in what format individuals will be given notice of consent [e.g., written notice, electronic notice, etc.])	Users that access the systems must reregister on an annual basis and any changes would be communicated through that process. NCI Investigators furnish their information to CTEP in a written application. IIF related to the Regulatory Support System (RSS)/Financial Management System (FMS) [JM1] are supplied to the CTSU at the time of account request via a standard application. Participating research organizations require trial participants to sign an authorization to use or disclose identifiable health information for research. A subject cannot enroll in a study without providing one of these release forms. They can withdraw the authorization at a later time, but then must leave the study. The link to the form is https://members.ctsu.org/readfile.asp?sectionid=1&fname=HIPAA/NSABP_HIPAA_Permission_030503.pdf&ftype=PDF
*32. Does the system host a website?:	Yes
*37. Does the website have any information or pages directed at children under the age of thirteen?:	No
*50. Are there policies or guidelines in place with regard to the retention and destruction of PII? (Refer to the C&A package and/or the Records Retention and Destruction section in SORN):	Yes
*54. Briefly describe in	CTSU data is maintained in a secure database.

detail how the PII will be secured on the system using administrative, technical, and physical controls.:	The following are in place as Management Controls: · Rules of Behavior · System Security Plan · Configuration Management, Change Management Plans and Processes · Disaster Recovery Plan · Interconnection Security Agreement The following are in place as Technical controls for CTSU: · User ID and Passwords are required to login to CTSU applications · The CTSU application is hosted within Westat Network boundaries and is protected by Westat provided Perimeter Firewall and Intrusion Detection Systems · SSL Encryption is enabled to access web based interfaces of CTSU modules, where necessary · Proactive Systems Monitoring and Alerts Management · Anti-virus, security updates and patching procedures · Periodic vulnerability scans for CTSU systems – both internal and external · Incidence Response Procedures · System and Database Audit Trails and Logs The following are in place as Operational controls for CTSU: · Personnel Security · Security Training/Clearance Process for all personnel working on CTSU · Westat Hiring and Termination Process · Non Disclosure Agreements for all employees working on CTSU · All employees take/review NIH CIT Security Awareness Training on an annual basis · Physical and Environmental Protection · Visitor Log Procedures · Backup Procedures · Offsite Storage for Tapes · Video Surveillance of Data Center · AC Maintenance Process · Contingency /Disaster Recovery Plan – tested regularly (last test on 11/2/08) · Incidence Response Procedures · Alerts and Scans · Identification and Authentication · User Account Management Process · Role based user access to systems · Password Change Policies (in sync with CTEP-ESYS)

- Procedures for handling lost/compromised passwords
- Audit Trails

Attachment 5

PIA REQUIRED INFORMATION

1 HHS Privacy Impact Assessment (PIA)

The PIA determines if Personally Identifiable Information (PII) is contained within a system, what kind of PII, what is done with that information, and how that information is protected. Systems with PII are subject to an extensive list of requirements based on privacy laws, regulations, and guidance. The HHS Privacy Act Officer may be contacted for issues related to Freedom of Information Act (FOIA) and the Privacy Act. Respective Operating Division (OPDIV) Privacy Contacts may be contacted for issues related to the Privacy Act. The Office of the Chief Information Officer (OCIO) can be used as a resource for questions related to the administrative, technical, and physical controls of the system. Please note that answers to questions with an asterisk (*) will be submitted to the Office of Management and Budget (OMB) and made publicly available in accordance with OMB Memorandum (M) 03-22.
Note: If a question or its response is not applicable, please answer "N/A" to that question where possible.

2 General Information

*Is this a new PIA?:	Yes
If this is an existing PIA, please provide a reason for revision:	
*1. Date of this Submission:	Feb 27, 2009
*2. OPDIV Name:	NIH
*3. Unique Project Identifier (UPI) Number for current fiscal year:	TBD
If the system does not have a UPI, please explain why it does not:	
*4. Privacy Act System of Records Notice (SORN) Number (If response to Q.21 is Yes, a SORN number is required for Q.4):	We are in the process of obtaining SOR Number
*5. OMB Information	TBD

Collection Approval Number: OMB Collection Approval Number Expiration Date: *6. Other Identifying Number(s):	TBD
*7. System Name: (Align with system item name)	NIH NCI Cancer Trials Support Unit (CTSU)
8. System Location: (OPDIV or contractor office building, room, city, and state)	

System Location:

OPDIV or contractor office building	Westat Inc.
Room	1650 Research Blvd.
City	Rockville
State	MD

*9. System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:	

Point of Contact Information

POC Name	Mike Montello

The following information will not be made publicly available:

POC Title	Associate Branch Chief for Clinical Trials Technology
POC Organization	NIH/NCI
POC Phone	301-435-9206
POC Email	montellom@mail.nih.gov

*10. Provide an	The Cancer Trials Support Unit (CTSU) is a service offered by the National

Attachment 5

overview of the system:	Cancer Institute to enhance and facilitate access to cancer clinical trials for clinical investigators in the United States and Canada. The CTSU maintains a broad menu of trials developed by the adult cancer Cooperative Groups and other research consortia and works with these organizations to offer patient enrollment, data collection, data quality management, and enrollment reimbursement services to clinical sites entering patients in these trials. In addition, the CTSU offers a regulatory support service to all adult cancer clinical trials by collection of regulatory documents and maintenance of a national database of investigators and sites. The CTSU also provides education and training for clinical site staff and clinical trials promotion services to help increase enrollment in cancer trials. A large and complex information technology infrastructure has been developed to support CTSU operations and exchange data with other data centers involved in cancer research. Westat is the prime contractor on the project, having two subcontractors, and working with numerous other organizations.

Attachment 5

SYSTEM CHARACTERIZATION AND DATA CATEGORIZATION

1 System Characterization and Data Configuration

11. Does HHS own the system?: If no, identify the system owner:	Yes
12. Does HHS operate the system?: If no, identify the system operator:	Yes
*13. Indicate if the system is new or an existing one being modified:	Existing
14. Identify the life-cycle phase of this system:	Operations/Maintenance
15. Have any of the following major changes occurred to the system since the PIA was last submitted?:	No

Please indicate “Yes” or “No” for each category below:	Yes/No
Conversions	
Anonymous to Non-Anonymous	
Significant System Management Changes	
Significant Merging	
New Public Access	
Commercial Sources	
New Interagency Uses	
Internal Flow or Collection	
Alteration in Character of Data	

16. Is the system a General Support System (GSS), Major Application (MA) or	Major Application

Minor Application?:	
*17. Does/Will the system collect, maintain (store), disseminate and/or pass through PII within any database(s), record(s), file(s) or website(s) hosted by this system?: Note: This question seeks to identify any, and all, personal information associated with the system. This includes any PII, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or whether it is personal information about business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation.	Yes

Please indicate "Yes" or "No" for each PII category. If the applicable PII category is not listed, please use the Other field to identify the appropriate category of PII.

Categories:	Yes/No
Name	Yes
Date of Birth	Yes
Social Security Number (SSN)	Yes

Photographic Identifiers	No
Driver’s License	No
Biometric Identifiers	No
Mother’s Maiden Name	No
Vehicle Identifiers	No
Mailing Address	Yes
Phone Numbers	Yes
Medical Records Numbers	Yes
Medical Notes	Yes
Financial Account Information	No
Certificates	No
Legal Documents	No
Device Identifiers	No
Web Uniform Resource Locator(s) (URL)	No
Email Address	Yes
Education Records	No
Military Status	No
Employment Status	No
Foreign Activities	No
Other	

18. Please indicate the categories of individuals about whom PII is collected, maintained, disseminated and/or passed through. Note: If the applicable PII category is not listed, please use the Other field to identify the appropriate category of PII. Please answer "Yes" or "No" to each of these choices (NA in other is not applicable).

Categories:	Yes/No
Employees	Yes
Public Citizen	No
Patients	Yes
Business partners/contacts (Federal, state, local agencies)	Yes
Vendors/Suppliers/Contractors	Yes
Other	NCI Investigators, NCI Associates, NCI Stakeholders

19. Are records on the system retrieved by one or more data elements?:	Yes

Please indicate "Yes" or "No" for each PII category. If the applicable PII category is not listed, please use the Other field to identify the appropriate category of PII.

Attachment 5

Categories:	Yes/No
Name	Yes
Date of Birth	No
SSN	No
Photographic Identifiers	No
Driver's License	No
Biometric Identifiers	No
Mother's Maiden Name	No
Vehicle Identifiers	No
Mailing Address	Yes
Phone Numbers	Yes
Medical Records Numbers	No
Medical Notes	No
Financial Account Information	No
Certificates	No
Legal Documents	No
Device Identifiers	No
Web URLs	No
Email Address	Yes
Education Records	No
Military Status	No
Employment Status	No
Foreign Activities	No
Other	

20. Are 10 or more records containing PII maintained, stored or transmitted/passed through this system?:	Yes
21. Is the system subject to the Privacy Act? (If response to Q.19 is Yes, response to Q.21 must be Yes and a SORN number is required for Q.4):	Yes
21 A. If yes, but a SORN has not been created, please provide an	

Attachment 5

explanation:

Attachment 5

INFORMATION SHARING PRACTICES

1 Information Sharing Practices

22. Does the system share or disclose PII with other divisions within this agency, external agencies, or other people or organizations outside the agency?:	Yes

Please indicate “Yes” or “No” for each category below:	Yes/No
Name	Yes
Date of Birth	Yes
SSN	Yes
Photographic Identifiers	No
Driver’s License	No
Biometric Identifiers	No
Mother’s Maiden Name	No
Vehicle Identifiers	No
Mailing Address	Yes
Phone Numbers	Yes
Medical Records Numbers	Yes
Medical Notes	Yes
Financial Account Information	No
Certificates	No
Legal Documents	No
Device Identifiers	No
Web URLs	No
Email Address	Yes
Education Records	No
Military Status	No
Employment Status	No
Foreign Activities	No
Other	

*23. If the system shares or discloses PII please specify with	CTSU shares NCI Investigator and NCI Associates data with CTEP-ESYS – a NCI sponsored project and other Cooperative Groups, to increase participation in NCI sponsored cancer related clinical trials.

whom and for what purpose(s):	With increased awareness and access to the trials information, CTEP intends to increase physician and patient participation in the NCI sponsored trials. CTSU shares this information, which may contain IIF, with lead research organizations for the purpose of assuring patient safety, for scientific decision making, drug distribution, regulatory oversight (i.e., investigator registration; trial audits) and to facilitate administrative operations. CTSU also shares this information with the Cooperative Groups and with NCI Center for Biomedical Informatics and Information Technology's Clinical Data System (CBIIT-CDS). Some of this information is available to staff at Cooperative Group member sites on a limited basis. Some of the information that CTSU shares with CTEP and CBIIT-CDS is also publicly available elsewhere.
24. If the PII in the system is matched against PII in one or more other computer systems, are computer data matching agreement(s) in place?:	Yes
25. Is there a process in place to notify organizations or systems that are dependent upon the PII contained in this system when major changes occur (i.e., revisions to PII, or when the system is replaced)?:	Yes
26. Are individuals notified how their PII is going to be used?:	Yes
If yes, please describe the process for allowing individu	CTSU obtains IIF related to NCI Investigators and Associates who are aware of the intended purpose and usage of the information. NCI Investigators furnish their information to CTEP in a written application. IIF related to the Regulatory Support System (RSS)/Financial Management System (FMS) [JM1] are supplied to the CTSU at the time of account request via a standard application. Participating research organizations require trial participants to sign an authorization to use or disclose identifiable health information for research. A subject cannot enroll

als to have a choice. If no, please provide an explanation:	in a study without providing one of these release forms. They can withdraw the authorization at a later time, but then must leave the study. The link to the form is https://members.ctsu.org/readfile.asp?sectionid=1&fname=HIPAA/NSABP_HIPAA_Permission_030503.pdf&ftype=PDF
27. Is there a complaint process in place for individuals who believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate?:	Yes
If yes, please describe briefly the notification process. If no, please provide an explanation:	Individuals can contact the CTSU Help Desk to make an incident report for release of IIF or for correction of IIF. A procedure document will be posted on the CTSU public web site.
28. Are there processes in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy?:	Yes
If yes, please describe briefly the review process. If no, please provide an explanation:	All NCI Investigator and Associate data are synchronized with the CTEP system. Data in that system are maintained through a yearly reregistration process that is required for both NCI Investigators and Associates. The CTSU member sites and the Cooperative Groups are contacted periodically for corrections to the IIF (e.g. name/email/phone) for their members who use the CTSU applications. The process and forms for maintaining patient related data are available as part of the protocols and can be submitted by the participating sites. Also, the quality assurance and audit procedures required are used to

	ensure accuracy of the data collected.
29. Are there rules of conduct in place for access to PII on the system?: Please indicate "Yes," "No," or "N/A" for each category. If yes, briefly state the purpose for each user to have access:	Yes

Users with access to PII	Yes/No/ N/A	Purpose
User	Yes	CTSU staff and Cooperative Groups: a) Maintain regulatory, membership, and protocol logistics data; b) Manage patient enrollment and clinical research data.
Administrators	Yes	Privileged CTSU staff: a) Manage system and provide support.
Developers	No	
Contractors	Yes	View/Update/Report Manage regulatory data.
Other		

*30. Please describe in detail: (1) the information the agency will collect, maintain, or disseminate; (2) why and for what purpose the agency will use the information; (3) in this description, explicitly indicate whether the information contains PII; and (4) whether submission of personal information is voluntary or mandatory:	Legislation authority is the Public Health Service Act (42 U.S.C. 241, 242, 248, 282, 284, 285a-j, 285l-q, 287, 287b, 287c, 289a, 289c, and 44 U.S.C. 3101.). The types of data used are scientific and health data about cancer clinical trials, including clinical and pre-clinical data with associated regulatory and administrative supporting information. Patient participation in CTEP clinical trials is voluntary and participants in CTEP clinical trials sign an informed consent. Types of information available in the CTSU Enterprise include protocols and protocol attributes, Investigator registration details, and non-IIF patient accrual details. The information is used to assure patient safety, for scientific decision making, drug distribution, regulatory oversight (i.e., investigator registration; trial audits) and to facilitate administrative operations. The CTSU collects and maintains various types of data. Investigator and treatment site staff information is obtained from the CTEP-ESYS and maintained in the CTSU. Cooperative Group staff use this data to maintain their membership rosters. This data is used as part of

	the credentialing requirements for patient enrollments. Protocol and regulatory information related to the member sites is collected and maintained in the CTSU Enterprise. This data is disseminated to Cooperative Groups to support patient enrollment and data collection processes. The CTSU also performs patient enrollments and will begin to collect demographic, eligibility criteria data, and other enrollment required data as part of this process. This data is collected on behalf of and shared with the organization that is leading a study. For some studies, the CTSU performs the complete data management and collects/maintains the clinical data collected for a study and disseminates it to the organization leading the study.
*31. Please describe in detail any processes in place to: (1) notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of the original collection); (2) notify and obtain consent from individuals regarding what PII is being collected from them; and (3) how the information will be used or shared. (Note: Please describe in what format individuals will be given notice of consent [e.g., written notice, electronic notice, etc.])	Users that access the systems must reregister on an annual basis and any char communicated through that process. CTSU obtains IIF related to NCI Investigators and Associates who are aware of purpose and usage of the information. NCI Investigators furnish their informat written application. IIF related to the Regulatory Support System (RSS)/Financ System (FMS) [JM1] are supplied to the CTSU at the time of account request v application. Participating research organizations require trial participants to sign an author disclose identifiable health information for research. A subject cannot enroll in providing one of these release forms. They can withdraw the authorization at then must leave the study. The link to the form is https://members.ctsu.org/re sectionid=1&fname=HIPAA/NSABP_HIPAA_Permission_030503.pdf&ftype=PD

Attachment 5

WEBSITE HOSTING PRACTICES

1 Website Hosting Practices

*32. Does the system host a website?:	Yes

Please indicate “Yes” or “No” for each type of site below:	Yes/ No
Internet	Yes
Intranet	Yes
Both	Yes

33. Is the website accessible by the public or other entities (i.e., Federal, state, and/or local agencies, contractors, third party administrators, etc.)?:	Yes
34. Is a website privacy policy statement (consistent with OMB M-03-22 and Title II and III of the E-Government Act) posted on the website?:	Yes
35. Is the website’s privacy policy in machine-readable format, such as Platform for Privacy Preferences (P3P)?:	No
If no, please indicate when the website will be P3P compliant:	March 2009
36. Does the website employ tracking technologies?:	Yes

Attachment 5

Please indicate “Yes”, “No”, or “N/A” for each type of cookies below:	Yes/No/N/A
Web Bugs	No
Web Beacons	No
Session Cookies	Yes
Persistent Cookies	No
Other	

*37. Does the website have any information or pages directed at children under the age of thirteen?:	No
If yes, is there a unique privacy policy for the site, and does the unique privacy policy address the process for obtaining parental consent if any information is collected?:	
38. Does the website collect PII from individuals?:	Yes

Please indicate “Yes” or “No” for each category below:	Yes/No
Name	Yes
Date of Birth	Yes
SSN	Yes
Photographic Identifiers	No
Driver's License	No
Biometric Identifiers	No
Mother's Maiden Name	No
Vehicle Identifiers	No
Mailing Address	Yes
Phone Numbers	Yes
Medical Records Numbers	Yes
Medical Notes	Yes
Financial Account Information	No
Certificates	No
Legal Documents	No

Device Identifiers	No
Web URLs	No
Email Address	Yes
Education Records	No
Military Status	No
Employment Status	No
Foreign Activities	No
Other	

39. Are rules of conduct in place for access to PII on the website?:	Yes
40. Does the website contain links to sites external to the OPDIV that owns and/or operates the system?:	No
If yes, note whether the system provides a disclaimer notice for users that follow external links to websites not owned or operated by the OPDIV.:	

Attachment 5

ADMINISTRATIVE CONTROLS

1 Administrative Controls
Note: This PIA uses the terms “Administrative,” “Technical” and “Physical” to refer to security control questions—terms that are used in several Federal laws when referencing security requirements.

2	
41. Has the system been certified and accredited (C&A)?:	No
41a. If yes, please indicate when the C&A was completed (Note: The C&A date is populated in the System Inventory form via the responsible Security personnel):	
41b. If a system requires a C&A and no C&A was completed, is a C&A in progress?:	Yes
42. Is there a system security plan for this system?:	Yes
43. Is there a contingency (or backup) plan for the system?:	Yes
44. Are files backed up regularly?:	Yes
45. Are backup files stored offsite?:	Yes
46. Are there user manuals for the system?:	Yes
47. Have personnel (system owners,	Yes

managers, operators, contractors and/or program managers) using the system been trained and made aware of their responsibilities for protecting the information being collected and maintained?:	
48. If contractors operate or use the system, do the contracts include clauses ensuring adherence to privacy provisions and practices?:	Yes
49. Are methods in place to ensure least privilege (i.e., “need to know” and accountability)?:	Yes
If yes, please specify method(s).:	There are user roles defined for CTSU Enterprise application access. These roles assure that those access privileges are very narrowly defined and that only the staff that perform these roles are granted that access. In addition to limiting functions, the user’s membership at sites also constrain the type of data that can be viewed. Accountability is assured through strict authentication and authorization and the use of audit logs that exist for applications, systems and network infrastructure components.
*50. Are there policies or guidelines in place with regard to the retention and destruction of PII? (Refer to the C&A package and/or the Records Retention and Destruction section in SORN):	Yes

If yes, please provide some detail about these policies/practices.:	IIF data stored in the CTSU is not purged or deleted and is retained to support CTSU'S business mission.

Attachment 5

TECHNICAL CONTROLS

1 Technical Controls

51. Are technical controls in place to minimize the possibility of unauthorized access, use, or dissemination of the data in the system?:	Yes

Please indicate “Yes” or “No” for each category below:	Yes/No
User Identification	Yes
Passwords	Yes
Firewall	Yes
Virtual Private Network (VPN)	Yes
Encryption	Yes
Intrusion Detection System (IDS)	Yes
Common Access Cards (CAC)	Yes
Smart Cards	No
Biometrics	No
Public Key Infrastructure (PKI)	Yes

52. Is there a process in place to monitor and respond to privacy and/or security incidents?:	Yes
If yes, please briefly describe the process:	Westat Systems Group is responsible for monitoring and responding to any security incident in collaboration with the CTSU project group. The Systems Group employs various tools such as Snort and regularly scheduled internal and external agency network vulnerability scans, etc., to stay on top of any security threat.

PHYSICAL ACCESS

1 Physical Access

53. Are physical access controls in place?:	Yes

Please indicate “Yes” or “No” for each category below:	Yes/No
Guards	Yes
Identification Badges	Yes
Key Cards	Yes
Cipher Locks	Yes
Biometrics	No
Closed Circuit TV (CCTV)	Yes

*54. Briefly describe in detail how the PII will be secured on the system using administrative, technical, and physical controls.:	CTSU data is maintained in a secure database. The following are in place as Management Controls: · Rules of Behavior · System Security Plan · Configuration Management, Change Management Plans and Processes · Disaster Recovery Plan · Interconnection Security Agreement The following are in place as Technical controls for CTSU: · User ID and Passwords are required to login to CTSU applications · The CTSU application is hosted within Westat Network boundaries and is protected by Westat provided Perimeter Firewall and Intrusion Detection Systems · SSL Encryption is enabled to access web based interfaces of CTSU modules, where necessary · Proactive Systems Monitoring and Alerts Management · Anti-virus, security updates and patching procedures · Periodic vulnerability scans for CTSU systems – both internal and external · Incidence Response Procedures · System and Database Audit Trails and Logs The following are in place as Operational controls for CTSU: · Personnel Security · Security Training/Clearance Process for all personnel working on CTSU

Attachment 5

· Westat Hiring and Termination Process
· Non Disclosure Agreements for all employees working on CTSU
· All employees take/review NIH CIT Security Awareness Training on an annual basis
· Physical and Environmental Protection
· Visitor Log Procedures
· Backup Procedures
· Offsite Storage for Tapes
· Video Surveillance of Data Center
· AC Maintenance Process
· Contingency /Disaster Recovery Plan – tested regularly (last test on 11/2/08)
· Incidence Response Procedures
· Alerts and Scans
· Identification and Authentication
· User Account Management Process
· Role based user access to systems
· Password Change Policies (in sync with CTEP-ESYS)
· Procedures for handling lost/compromised passwords
· Audit Trails

The system falls under the Privacy Act System of Records Notice 09-25-0200

Attachment 5

APPROVAL/DEMOTION

1 System Information

System Name:	NIH NCI Cancer Trials Support Unit (CTSU)

2 PIA Reviewer Approval/Promotion or Demotion

Promotion/Demotion:	
Comments:	
Approval/Demotion Point of Contact:	
Date:	Feb 27, 2009

3 Senior Official for Privacy Approval/Promotion or Demotion

Promotion/Demotion:	
Comments:	

4 OPDIV Senior Official for Privacy or Designee Approval

Please print the PIA and obtain the endorsement of the reviewing official below. Once the signature has been collected, retain a hard copy for the OPDIV's records. Submitting the PIA will indicate the reviewing official has endorsed it

This PIA has been reviewed and endorsed by the OPDIV Senior Official for Privacy or Designee (Name and Date):

Name: _____ Date: _____

Name:

Date:

5 Department Approval to Publish to the Web

Approved for web publishing

Date Published:

Publicly posted PIA URL or no PIA URL explanation:

Attachment 5

% COMPLETE

1 PIA Completion

PIA Percentage Complete:	100.00
PIA Missing Fields:	