Standard Operating Procedure (SOP)
BRICS System Access Logs

Document Information

Document Owners: Matthew McAuliffe, Yang Fann, and Dominic Nathan

Organizations: NINDS DIR ITBP, CIT OIR ISL BIRSS, CNRM

Approval / Distribution Process

The SOP approval/distribution process is as follows:

1. The SOP author sends the SOP SharePoint link to their peers/subject matter experts (SMEs) for review.
2. After editing, the SOP author decides whether the SOP is ready for approval. If the SOP is ready, the author adds the SOP to the ITBP Manager meeting agenda.
3. At the ITBP Managers meeting or via email, NINDS Management formally approves/disapproves the SOP.
4. The SOP Author sends the SOP link to all people on the Distribution List.

NINDS Approval

This Standard Operating Procedure (SOP) is approved for distribution and implementation as of the Director ITBP approval date listed below. NINDS ITBP management is authorized to conduct periodic audits to ensure compliance with this procedure. Requests for corrections or changes to any part of this procedure must be submitted to the Document Owner to review. Exceptions to any procedure must be approved by the ITBP Management and documented.

Approved By:

Name	Title	Organization	Approval Date
Yang Fann	IT Director	NINDS DIR ITBP	03/28/19
Matthew McAuliffe	BIRSS Chief	CIT OIR ISL BIRSS	03/28/19

Name	Title	Organization	Approval Date
Dominic Nathan	Informatics Core Director	CNRM	03/28/19
Mark Edwards	IT Manager	NINDS DIR ITBP	03/28/19
Willy Calderon	ISSO	NINDS DIR ITBP	03/28/19

Peer Reviewers

This Standard Operating Procedure was reviewed by the peers (i.e., subject matter experts) listed below. The procedure will be reviewed by the peer reviewers at least annually.

Reviewed By:

Name	Title	Organization	Date
Tsega Gabremichael	Team Lead	CIT OIR ISL BIRSS	03/27/19
Leonie Misquitta	Sr Scientific Advisor	CIT OIR ISL BIRSS	03/27/19
Dominic Nathan	Informatics Core Director	CNRM	03/27/19

Distribution List

This Standard Operating Procedure impacts the individuals on this Distribution List. The SOP author should notify everyone on this list about changes to this SOP *within one week* of NINDS approval.

Distributed To:

Name / Department / Group / Team
Yang Fann
Matthew McAuliffe
Dominic Nathan
Willy Calderon

1. Introduction

1.1 Overview

This document presents the Standard Operating Procedure for managing BRICS system event, access logging, and audit trails. The intended audience for this procedure includes the groups/individuals listed below:

- NINDS DIR Clinical Informatics Development Team
- CIT OIR ISL BIRSS Development Team

NINDS also developed the Application Security Auditing SOP to satisfy the NIST 800-53 security control requirement(s) stated below:

- AU-1, Audit and Accountability Policy and Procedures
- AU-2, Auditable Events
- AU-3, Content of Audit Records
- AU-4, Audit Storage Capacity
- AU-5, Audit Processing
- AU-6, Audit Monitoring, Analysis and Reporting
- AU-7, Audit Reduction and Report Generation
- AU-8, Time Stamps
- AU-9, Protection of Audit Information
- AU-10, Non-repudiation
- AU-11, Audit Retention

1.2 Purpose

This Standard Operating Procedure documents the standards that are in place to meet FDA regulations for system logs of the BRICS and its associated systems such as CiSTAR, CASA, and ProFoRMS at NINDS, CIT and CNRM.

1.3 Scope

This Standard Operating Procedure applies to system logs of custom applications that are 21 CFR Part 11 compliant.

1.4 Roles and Responsibilities

The following table defines the roles and responsibilities and also serves as the list of points of contact for issues and concerns relating to the BRICS system logs.

Name	Title	Responsibility
Clinical Trial Unit	NINDS DIR CTU	NINDS Governance committee for approvals
Steering Committee	Informatics Core	CNRM Governance committee for approvals
Yang Fann	BRICS Co-Director NINDS IT Director	Authorizing Official to operate Approve requirements
Matthew McAuliffe	BRICS Co-Director CIT BIRSS Chief	Approve requirements
Dominic Nathan	Informatics Core Director	Manage the project
Leonie Misquitta	Sr Scientific Advisor	Provide scientific consulting
Tsega Gebremichael	Sr Software Engineer	Provide technical guidance
Change Control Board	Subject Matter Experts	Manage and approve change requests and system enhancements
Business, Product owner, Instance Program Manager	Key Stakeholders	Review and validate requirements and work products
NINDS/CIT Clinical Informatics Development team	Software Engineer	Responsible for understanding and following the scrum development processes outlined in this document.

1.5 Definitions

The following definition may assist in understanding this SOP.

- HIPAA – Health Insurance Portability and Accountability Act of 1996
- BRICS – Biomedical Research Informatics Computing System

- CiSTAR – Clinical Informatics System for Trials and Research
- CASA – Collection Access Sharing Analytics Platform
- CNRM – Center for Neuroscience and Regenerative Medicine

1.6 Key Words

The following key terms are used in this SOP.

- Access logs
- Audit trails

2. Application Logs

In some cases, many NINDS applications generate their own log files, while others use the logging capabilities of the OS on which they are installed. Applications vary significantly in the types of information that they log. The following lists some of the most commonly logged types of information and the potential benefits of each. There is a baseline security logging solution that has been created by the NINDS Application Development team to be used by all NINDS applications to address security requirements. These are applications defined with Federal Information Processing Standards (FIPS) 199 impact levels as *low*, *medium,* or *high*.

- **Client requests and server responses**, which can be very helpful in reconstructing sequences of events and determining their apparent outcome. If the application logs successful user authentications, it is usually possible to determine which user made each request. Some applications can perform highly detailed logging, such as email servers recording the sender, recipients, subject name, and attachment names for each email; Web servers recording each URL requested and the type of response provided by the server; and business applications recording which financial records were accessed by each user. This information can be used to identify or investigate incidents and to monitor application usage for compliance and auditing purposes.
- **Account information** such as successful and failed authentication attempts, account changes (e.g., account creation and deletion; account privilege assignment), and use of privileges. In addition to identifying security events such as brute force password guessing and escalation of privileges, it can be used to identify who has used the application and when each person has used it.

- **Usage information** such as the number of transactions occurring in a certain period (e.g., minute, hour) and the size of transactions (e.g., email message size, file transfer size). This can be useful for certain types of security monitoring (e.g., a ten-fold increase in email activity might indicate a new email-borne malware threat; an unusually large outbound email message might indicate inappropriate release of information).

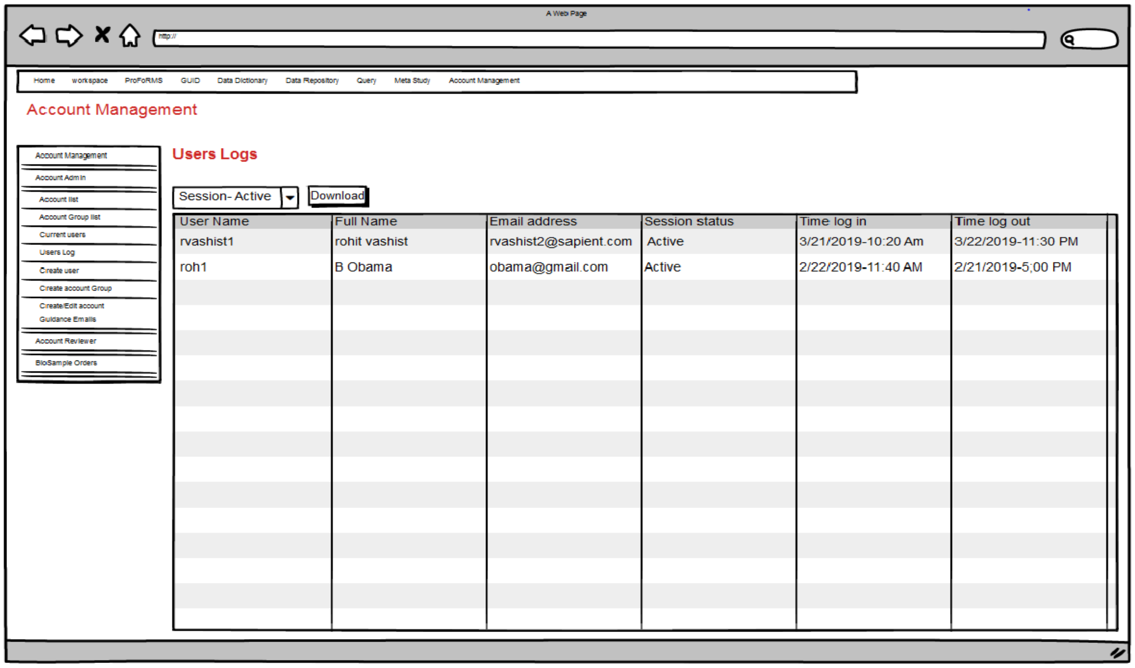
- **Significant operational actions** such as application startup and shutdown, application failures, and major application configuration changes. This can be used to identify security compromises and operational failures.

2.1 Application Security Logging

Baseline application security for applications classified as *Low*, *Medium*, *High* impact levels. Currently there is no application classified with a *High* impact level at NINDS DIR ITBP. NINDS applications use the following approaches to capture key events to monitor and identify security issues.

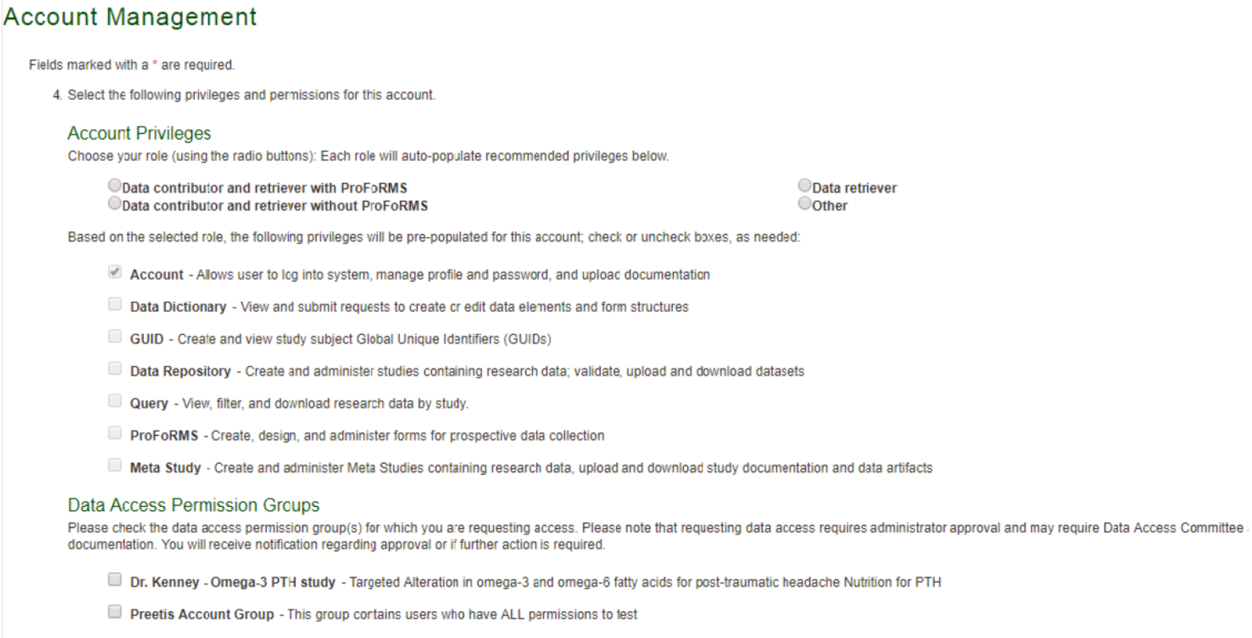
Implementation:

1. **Functional Requirement – Users Logs**



User Name	Full Name	Email address	Session status	Time log in	Time log out
rvashist1	rohit vashist	rvashist2@sapient.com	Active	3/21/2019-10:20 Am	3/22/2019-11:30 PM
roh1	B Obama	obama@gmail.com	Active	2/22/2019-11:40 AM	2/21/2019-5;00 PM

The Account Management is for creating, approving, and managing user accounts, including management of access controls, roles, permissions groups, and authorization to other BRICS modules. The Users Logs track the user name, full name, email addression, session status, time logging in and out.



Account Management

Fields marked with a * are required.

4. Select the following privileges and permissions for this account.

Account Privileges

Choose your role (using the radio buttons): Each role will auto-populate recommended privileges below.

○ **Data contributor and retriever with ProFoRMS**
○ **Data contributor and retriever without ProFoRMS**
○ **Data retriever**
○ **Other**

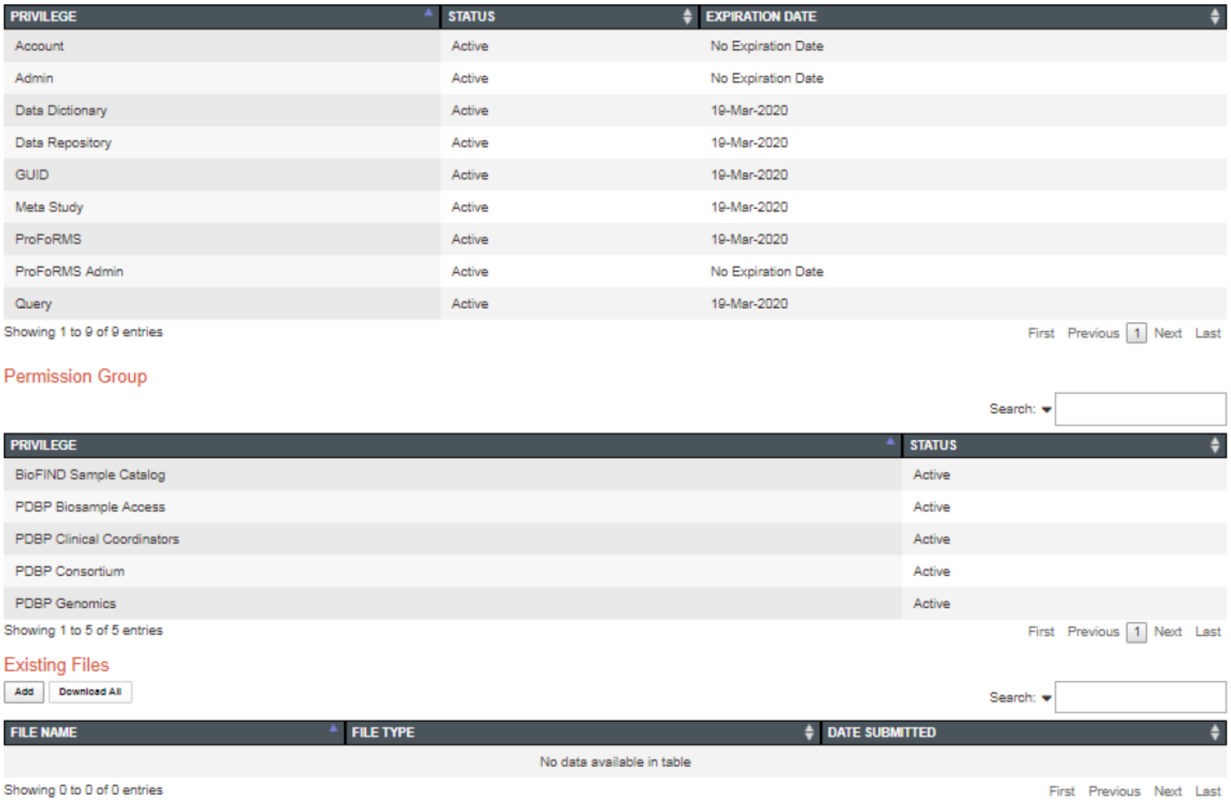
Based on the selected role, the following privileges will be pre-populated for this account; check or uncheck boxes, as needed:

- ☑ **Account** - Allows user to log into system, manage profile and password, and upload documentation
- ☐ **Data Dictionary** - View and submit requests to create or edit data elements and form structures
- ☐ **GUID** - Create and view study subject Global Unique Identifiers (GUIDs)
- ☐ **Data Repository** - Create and administer studies containing research data; validate, upload and download datasets
- ☐ **Query** - View, filter, and download research data by study.
- ☐ **ProFoRMS** - Create, design, and administer forms for prospective data collection
- ☐ **Meta Study** - Create and administer Meta Studies containing research data, upload and download study documentation and data artifacts

Data Access Permission Groups

Please check the data access permission group(s) for which you are requesting access. Please note that requesting data access requires administrator approval and may require Data Access Committee documentation. You will receive notification regarding approval or if further action is required.

- ☐ **Dr. Kenney - Omega-3 PTH study** - Targeted Alteration in omega-3 and omega-6 fatty acids for post-traumatic headache Nutrition for PTH
- ☐ **Preetis Account Group** - This group contains users who have ALL permissions to test



PRIVILEGE	STATUS	EXPIRATION DATE
Account	Active	No Expiration Date
Admin	Active	No Expiration Date
Data Dictionary	Active	19-Mar-2020
Data Repository	Active	19-Mar-2020
GUID	Active	19-Mar-2020
Meta Study	Active	19-Mar-2020
ProFoRMS	Active	19-Mar-2020
ProFoRMS Admin	Active	No Expiration Date
Query	Active	19-Mar-2020

Showing 1 to 9 of 9 entries

Permission Group

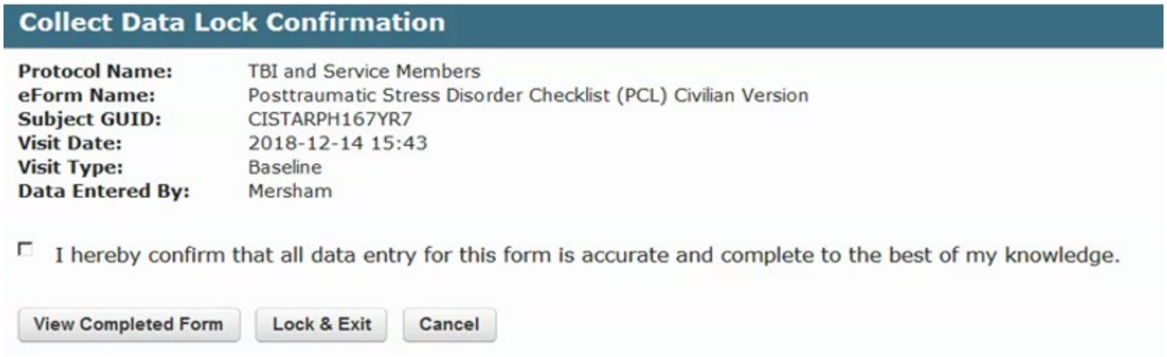
PRIVILEGE	STATUS
BioFIND Sample Catalog	Active
PDBP Biosample Access	Active
PDBP Clinical Coordinators	Active
PDBP Consortium	Active
PDBP Genomics	Active

Showing 1 to 5 of 5 entries

Existing Files

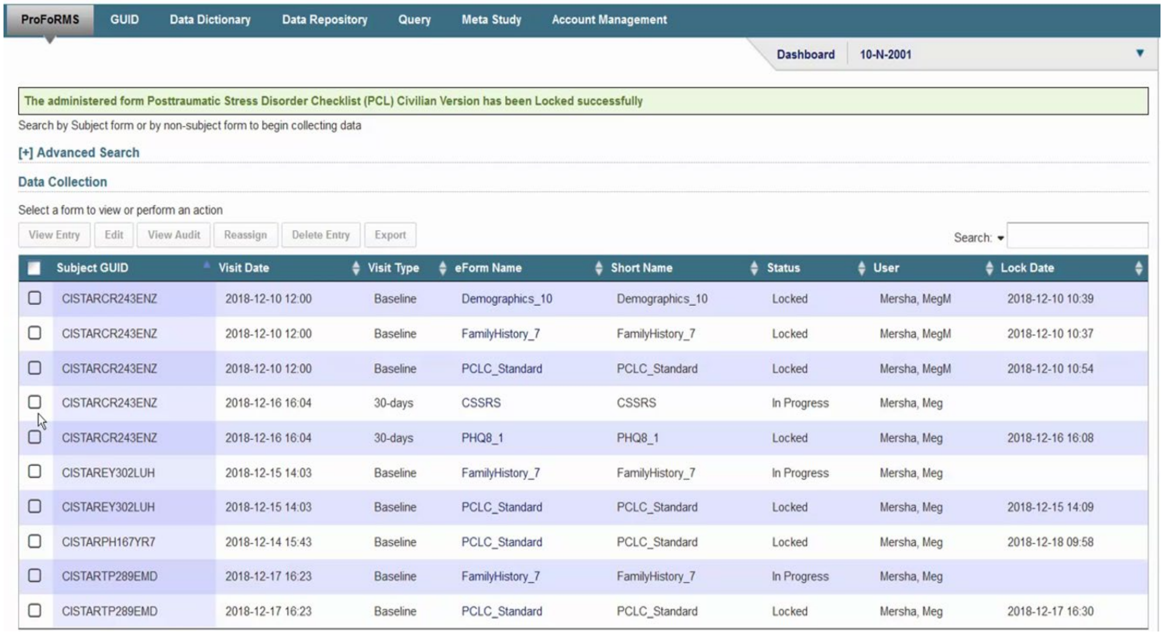
FILE NAME	FILE TYPE	DATE SUBMITTED
No data available in table		

Showing 0 to 0 of 0 entries



Protocol Name:	TBI and Service Members
eForm Name:	Posttraumatic Stress Disorder Checklist (PCL) Civilian Version
Subject GUID:	CISTARPH167YR7
Visit Date:	2018-12-14 15:43
Visit Type:	Baseline
Data Entered By:	Mersham

☐ I hereby confirm that all data entry for this form is accurate and complete to the best of my knowledge.

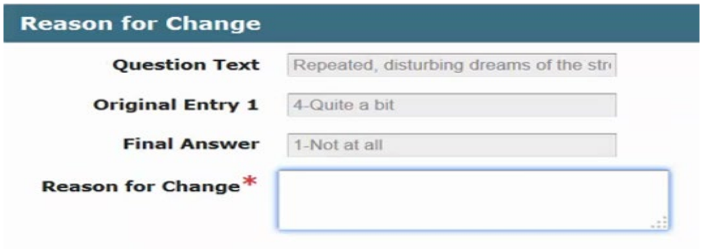


The administered form Posttraumatic Stress Disorder Checklist (PCL) Civilian Version has been Locked successfully

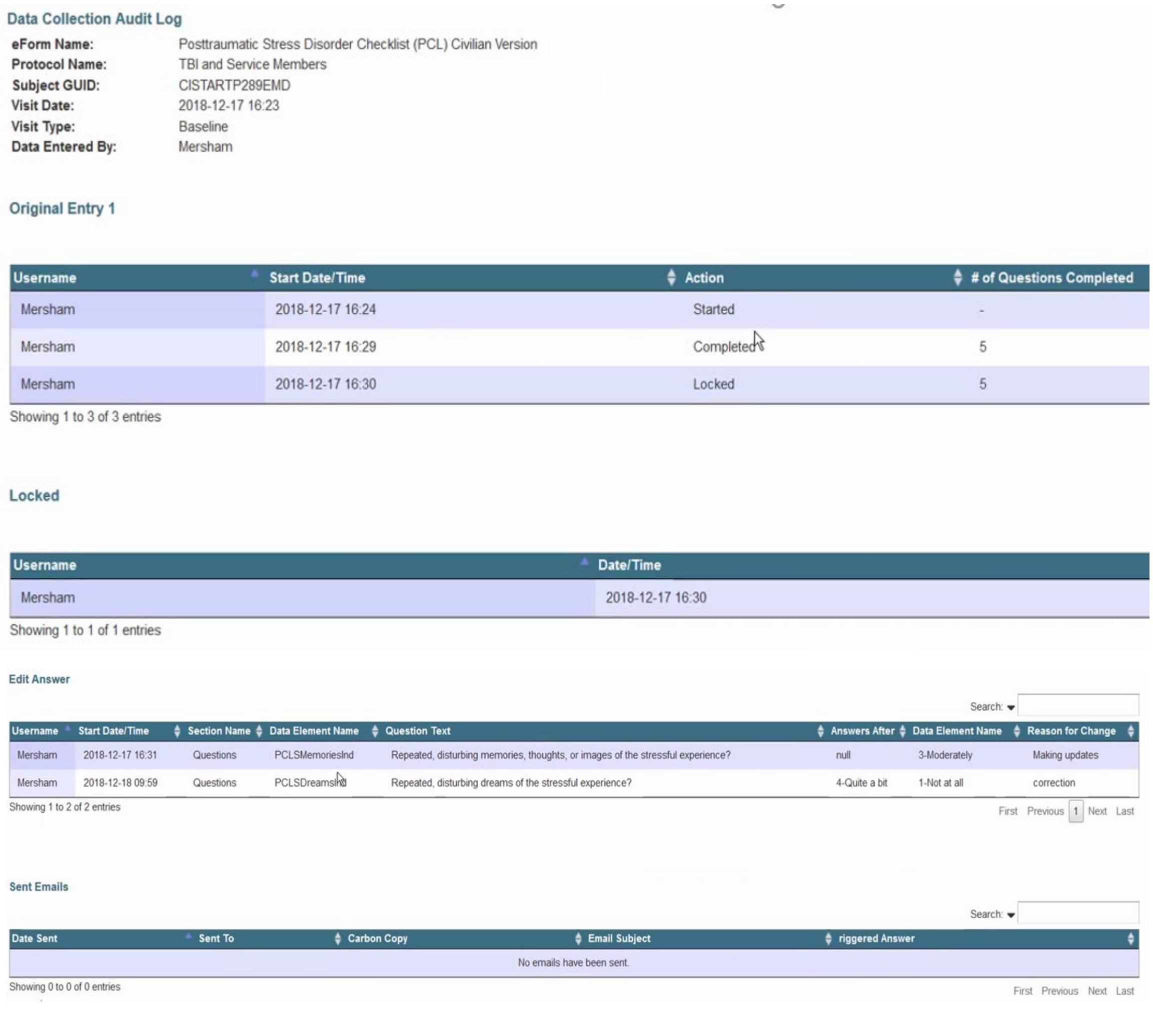
Search by Subject form or by non-subject form to begin collecting data

Select a form to view or perform an action

☐	Subject GUID	Visit Date	Visit Type	eForm Name	Short Name	Status	User	Lock Date
☐	CISTARCR243ENZ	2018-12-10 12:00	Baseline	Demographics_10	Demographics_10	Locked	Mersha, MegM	2018-12-10 10:39
☐	CISTARCR243ENZ	2018-12-10 12:00	Baseline	FamilyHistory_7	FamilyHistory_7	Locked	Mersha, MegM	2018-12-10 10:37
☐	CISTARCR243ENZ	2018-12-10 12:00	Baseline	PCLC_Standard	PCLC_Standard	Locked	Mersha, MegM	2018-12-10 10:54
☐	CISTARCR243ENZ	2018-12-16 16:04	30-days	CSSRS	CSSRS	In Progress	Mersha, Meg	
☐	CISTARCR243ENZ	2018-12-16 16:04	30-days	PHQ8_1	PHQ8_1	Locked	Mersha, Meg	2018-12-16 16:08
☐	CISTAREY302LUH	2018-12-15 14:03	Baseline	FamilyHistory_7	FamilyHistory_7	In Progress	Mersha, Meg	
☐	CISTAREY302LUH	2018-12-15 14:03	Baseline	PCLC_Standard	PCLC_Standard	Locked	Mersha, Meg	2018-12-15 14:09
☐	CISTARPH167YR7	2018-12-14 15:43	Baseline	PCLC_Standard	PCLC_Standard	Locked	Mersha, Meg	2018-12-18 09:58
☐	CISTARTP289EMD	2018-12-17 16:23	Baseline	FamilyHistory_7	FamilyHistory_7	In Progress	Mersha, Meg	
☐	CISTARTP289EMD	2018-12-17 16:23	Baseline	PCLC_Standard	PCLC_Standard	Locked	Mersha, Meg	2018-12-17 16:30



Question Text	Repeated, disturbing dreams of the str
Original Entry 1	4-Quite a bit
Final Answer	1-Not at all
Reason for Change*	



Data Collection Audit Log

eForm Name:	Posttraumatic Stress Disorder Checklist (PCL) Civilian Version
Protocol Name:	TBI and Service Members
Subject GUID:	CISTARTP289EMD
Visit Date:	2018-12-17 16:23
Visit Type:	Baseline
Data Entered By:	Mersham

Original Entry 1

Username	Start Date/Time	Action	# of Questions Completed
Mersham	2018-12-17 16:24	Started	-
Mersham	2018-12-17 16:29	Completed	5
Mersham	2018-12-17 16:30	Locked	5

Showing 1 to 3 of 3 entries

Locked

Username	Date/Time
Mersham	2018-12-17 16:30

Showing 1 to 1 of 1 entries

Edit Answer

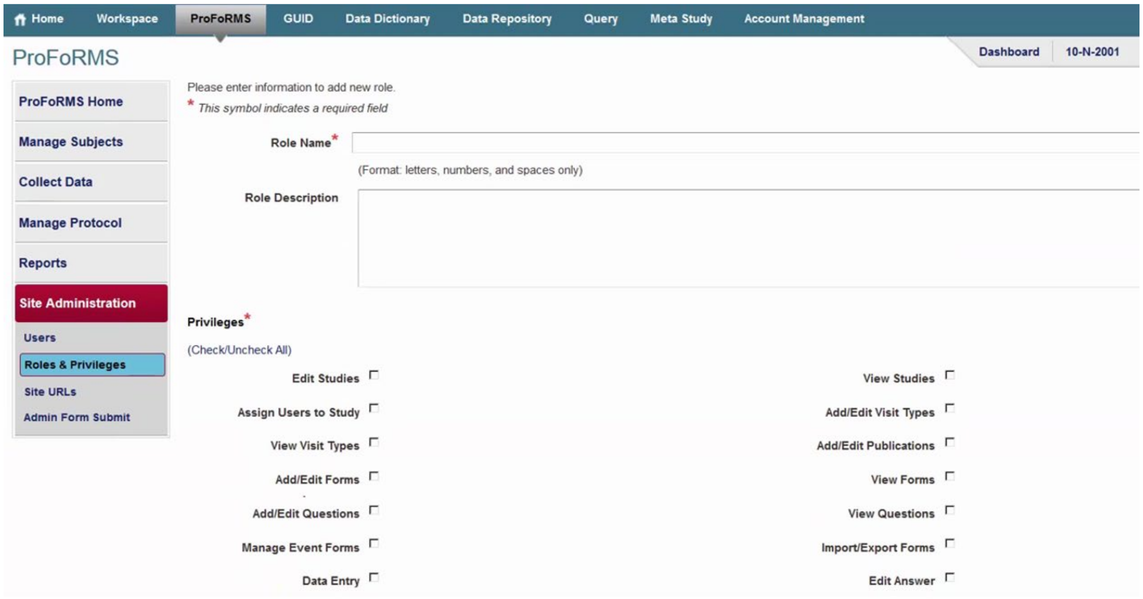
Username	Start Date/Time	Section Name	Data Element Name	Question Text	Answers After	Data Element Name	Reason for Change
Mersham	2018-12-17 16:31	Questions	PCLSMemoriesInd	Repeated, disturbing memories, thoughts, or images of the stressful experience?	null	3-Moderately	Making updates
Mersham	2018-12-18 09:59	Questions	PCLSDreamsInd	Repeated, disturbing dreams of the stressful experience?	4-Quite a bit	1-Not at all	correction

Showing 1 to 2 of 2 entries

Sent Emails

Date Sent	Sent To	Carbon Copy	Email Subject	riggered Answer
No emails have been sent.				

Showing 0 to 0 of 0 entries



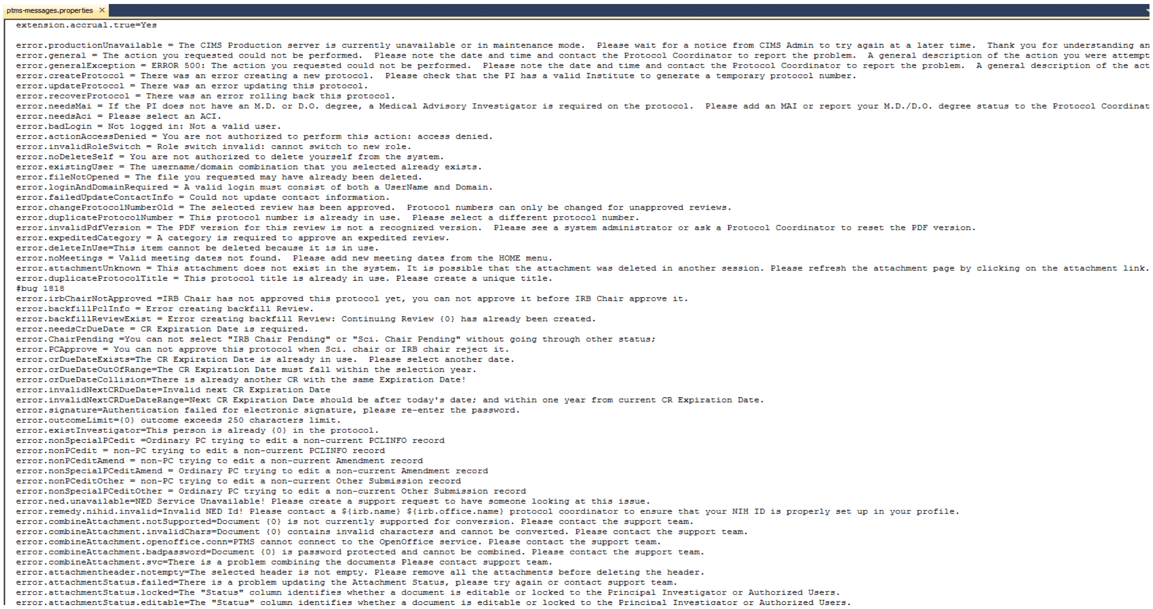
Please enter information to add new role.
* *This symbol indicates a required field*

Role Name*
(Format: letters, numbers, and spaces only)
Role Description

Privileges*
(Check/Uncheck All)

- Edit Studies ☐
- Assign Users to Study ☐
- View Visit Types ☐
- Add/Edit Forms ☐
- Add/Edit Questions ☐
- Manage Event Forms ☐
- Data Entry ☐
- View Studies ☐
- Add/Edit Visit Types ☐
- Add/Edit Publications ☐
- View Forms ☐
- View Questions ☐
- Import/Export Forms ☐
- Edit Answer ☐

2. **System Tracking Framework –** NINDS applications use the standard error tags to collect important application activities and to allow the team to monitor and react to events as well as to be used in investigation of unexpected or unauthorized activity.

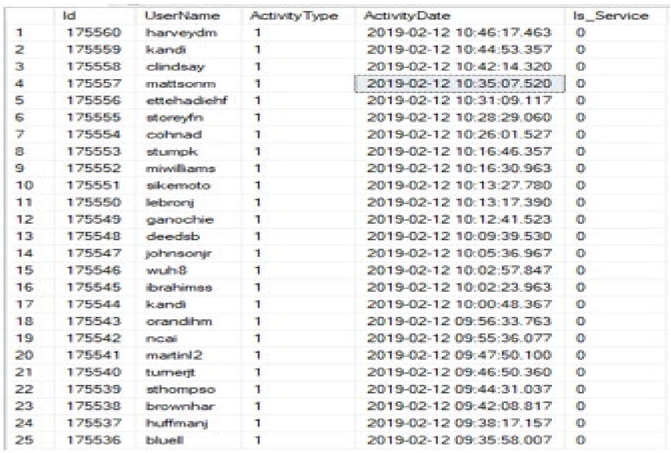


```
extension.accrual.true=Yes

error.productionUnavailable = The CIMS Production server is currently unavailable or in maintenance mode.  Please wait for a notice from CIMS Admin to try again at a later time.  Thank you for understanding an
error.general = The action you requested could not be performed.  Please note the date and time and contact the Protocol Coordinator to report the problem.  A general description of the action you were attempt
error.generalException = ERROR 500: The action you requested could not be performed.  Please note the date and time and contact the Protocol Coordinator to report the problem.  A general description of the act
error.createProtocol = There was an error creating a new protocol.  Please check that the PI has a valid Institute to generate a temporary protocol number.
error.updateProtocol = There was an error updating this protocol.
error.recoverProtocol = There was an error rolling back this protocol.
error.needsMai = If the PI does not have an M.D. or D.O. degree, a Medical Advisory Investigator is required on the protocol.  Please add an MAI or report your M.D./D.O. degree status to the Protocol Coordinat
error.needsAci = Please select an ACI.
error.badLogin = Not logged in: Not a valid user.
error.actionAccessDenied = You are not authorized to perform this action: access denied.
error.invalidRoleSwitch = Role switch invalid: cannot switch to new role.
error.noDeleteSelf = You are not authorized to delete yourself from the system.
error.existingUser = The username/domain combination that you selected already exists.
error.fileNotOpened = The file you requested may have already been deleted.
error.loginAndDomainRequired = A valid login must consist of both a UserName and Domain.
error.failedUpdateContactInfo = Could not update contact information.
error.changeProtocolNumberOld = The selected review has been approved.  Protocol numbers can only be changed for unapproved reviews.
error.duplicateProtocolNumber = This protocol number is already in use.  Please select a different protocol number.
error.invalidPdfVersion = The PDF version for this review is not a recognized version.  Please see a system administrator or ask a Protocol Coordinator to reset the PDF version.
error.expeditedCategory = A category is required to approve an expedited review.
error.deleteInUse=This item cannot be deleted because it is in use.
error.noMeetings = Valid meeting dates not found.  Please add new meeting dates from the HOME menu.
error.attachmentUnknown = This attachment does not exist in the system. It is possible that the attachment was deleted in another session. Please refresh the attachment page by clicking on the attachment link.
error.duplicateProtocolTitle = This protocol title is already in use. Please create a unique title.
#bug 1818
error.irbChairNotApproved =IRB Chair has not approved this protocol yet, you can not approve it before IRB Chair approve it.
error.backfillPclInfo = Error creating backfill Review.
error.backfillReviewExist = Error creating backfill Review: Continuing Review {0} has already been created.
error.needsCrDueDate = CR Expiration Date is required.
error.ChairPending =You can not select "IRB Chair Pending" or "Sci. Chair Pending" without going through other status;
error.PCApprove = You can not approve this protocol when Sci. chair or IRB chair reject it.
error.crDueDateExists=The CR Expiration Date is already in use.  Please select another date.
error.crDueDateOutOfRange=The CR Expiration Date must fall within the selection year.
error.crDueDateCollision=There is already another CR with the same Expiration Date!
error.invalidNextCRDueDate=Invalid next CR Expiration Date
error.invalidNextCRDueDateRange=Next CR Expiration Date should be after today's date; and within one year from current CR Expiration Date.
error.signature=Authentication failed for electronic signature, please re-enter the password.
error.outcomeLimit={0} outcome exceeds 250 characters limit.
error.existInvestigator=This person is already {0} in the protocol.
error.nonSpecialPCedit =Ordinary PC trying to edit a non-current PCLINFO record
error.nonPCedit = non-PC trying to edit a non-current PCLINFO record
error.nonPCeditAmend = non-PC trying to edit a non-current Amendment record
error.nonSpecialPCeditAmend = Ordinary PC trying to edit a non-current Amendment record
error.nonPCeditOther = non-PC trying to edit a non-current Other Submission record
error.nonSpecialPCeditOther = Ordinary PC trying to edit a non-current Other Submission record
error.ned.unavailable=NED Service Unavailable! Please create a support request to have someone looking at this issue.
error.remedy.nihid.invalid=Invalid NED Id! Please contact a ${irb.name} ${irb.office.name} protocol coordinator to ensure that your NIH ID is properly set up in your profile.
error.combineAttachment.notSupported=Document {0} is not currently supported for conversion. Please contact the support team.
error.combineAttachment.invalidChars=Document {0} contains invalid characters and cannot be converted. Please contact the support team.
error.combineAttachment.openoffice.conn=PTMS cannot connect to the OpenOffice service. Please contact the support team.
error.combineAttachment.badpassword=Document {0} is password protected and cannot be combined. Please contact the support team.
error.combineAttachment.svc=There is a problem combining the documents Please contact support team.
error.attachmentheader.notempty=The selected header is not empty. Please remove all the attachments before deleting the header.
error.attachmentStatus.failed=There is a problem updating the Attachment Status, please try again or contact support team.
error.attachmentStatus.locked=The "Status" column identifies whether a document is editable or locked to the Principal Investigator or Authorized Users.
error.attachmentStatus.editable=The "Status" column identifies whether a document is editable or locked to the Principal Investigator or Authorized Users.
```

System tracking includes:

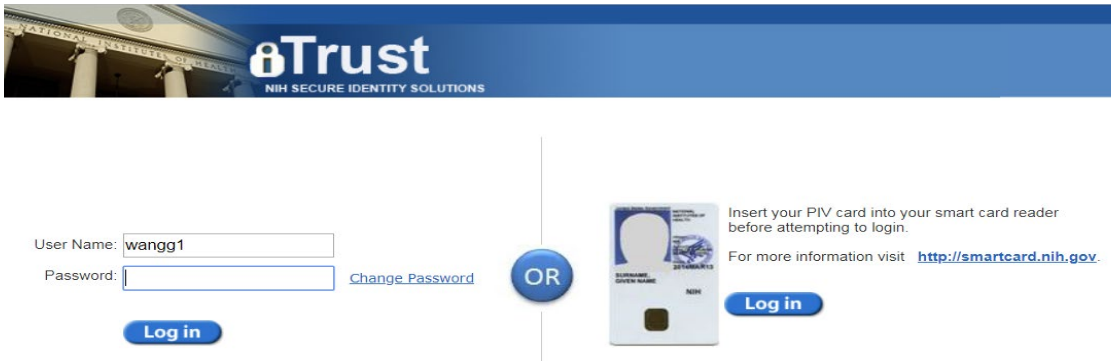
a. Activity information logging after a user passes NIH login screen.



	Id	UserName	ActivityType	ActivityDate	Is_Service
1	175560	harveydm	1	2019-02-12 10:46:17.463	0
2	175559	kandi	1	2019-02-12 10:44:53.357	0
3	175558	clindsay	1	2019-02-12 10:42:14.320	0
4	175557	mattsonm	1	2019-02-12 10:35:07.520	0
5	175556	ettehadiehf	1	2019-02-12 10:31:09.117	0
6	175555	storeyfn	1	2019-02-12 10:28:29.060	0
7	175554	cohnad	1	2019-02-12 10:26:01.527	0
8	175553	stumpk	1	2019-02-12 10:16:46.357	0
9	175552	miwilliams	1	2019-02-12 10:16:30.963	0
10	175551	sikemoto	1	2019-02-12 10:13:27.780	0
11	175550	lebronj	1	2019-02-12 10:13:17.390	0
12	175549	ganochie	1	2019-02-12 10:12:41.523	0
13	175548	deedsb	1	2019-02-12 10:09:39.530	0
14	175547	johnsonjr	1	2019-02-12 10:05:36.967	0
15	175546	wuh8	1	2019-02-12 10:02:57.847	0
16	175545	ibrahimss	1	2019-02-12 10:02:23.963	0
17	175544	kandi	1	2019-02-12 10:00:48.367	0
18	175543	orandihm	1	2019-02-12 09:56:33.763	0
19	175542	ncai	1	2019-02-12 09:55:36.077	0
20	175541	martinl2	1	2019-02-12 09:47:50.100	0
21	175540	turnerjt	1	2019-02-12 09:46:50.360	0
22	175539	sthompso	1	2019-02-12 09:44:31.037	0
23	175538	brownhar	1	2019-02-12 09:42:08.817	0
24	175537	huffmanj	1	2019-02-12 09:38:17.157	0
25	175536	bluell	1	2019-02-12 09:35:58.007	0

b. Logging Application Exception when exceptions are triggered.

c. Login security policy enforcement with NIH Login.



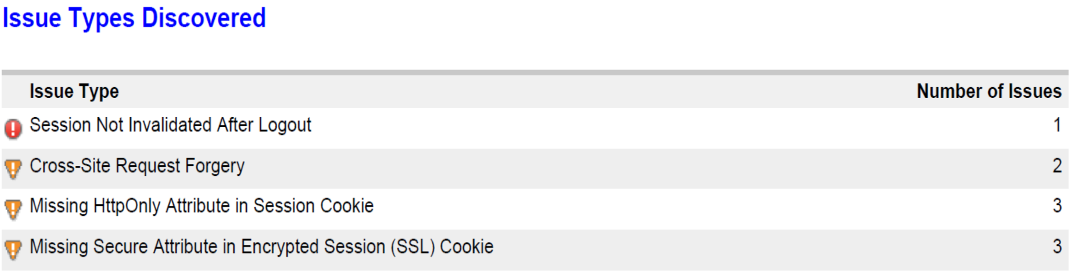
User Name: wangg1

Password:

Insert your PIV card into your smart card reader before attempting to login.

For more information visit http://smartcard.nih.gov.

d. Appscan Security Issues reports



Issue Types Discovered

Issue Type	Number of Issues
Session Not Invalidated After Logout	1
Cross-Site Request Forgery	2
Missing HttpOnly Attribute in Session Cookie	3
Missing Secure Attribute in Encrypted Session (SSL) Cookie	3

Reports are reviewed by the security team and by the application team before production deployments.

3. **Supporting Infrastructure Logging and Monitoring** – System level logging and monitoring is critical for providing a multi-level security framework. The following are external controls that are in place to complete NINDS's application security framework.

   - **Monitoring of server and services that host the application** – Key monitors are in place to make sure the environment supporting each application is up and working properly. Issues are flagged and addressed by the Network Operations Team.

   - **Website log files** – All application sites have log files enabled to capture information about application connections and page visits.

   - **Databases in full recovery mode** – All NINDS application databases are placed into full recovery mode to collect information at the database transaction level. The transactional data can be used to replay transactions and restore the database to a specific point in time for data-related security investigations. Database backup and transaction logs are kept for a minimum of 90 days.

- **Database Monitoring** – All application databases are monitored to alert on key events such failed database logins, disk space, and performance issues that may indicate unusual activity.
- **Website monitoring** – Used to confirm if the site is up and accessible.

*All logs will be kept for a minimum of 30 days and for most purposes will continue to be logged well after 30 days in a central repository before handing off to the SOC for further archiving.

3. System Access Logs

All servers maintain system logs in the /var/log directory and this directory is only viewable by the system admins. The logs are archived every week and kept for a minimum of one month. In addition, the admins can see who is logged in at any given time and a history of all successful or unsuccessful logins.

Below is the process for the system admins to manage the details about these log files:

1) System admin logins to the server(s) using secure Two-factor Authentication (2FA).
2) The Admin sudo’s as the root user (that requires 2FA).
3) Admin user views the /var/log/secure file using a text editor and navigates to the bottom of the file for the most recent date.
4) The system logs capture the following information:

    a) Username
    b) IP address for source machine
    c) Login method
    d) Time log In - (Date and time)
    e) Time log Out- (Date and time)

3.1 Operating System Logging

There are certain security-level event auditing items that are done outside of the application to meet basic security needs. Operating systems (OS) for servers, workstations, and networking devices (e.g., routers, switches) usually log a variety of information related to security. The most common types of security-related OS data are as follows:

- **System Events.** System events are operational actions performed by OS components, such as shutting down the system or starting a service. Typically, failed events and the most significant successful events are logged, but many OSs permit administrators to specify which types of events will be logged. The details logged for each event also vary widely; each event is usually timestamped, and other supporting information could include event, status, and error codes; service name; and user or system account associated with an event.
- **Audit Records.** Audit records contain security event information such as successful and failed authentication attempts, file accesses, security policy changes, account changes (e.g., account creation and deletion, account privilege assignment), and use of privileges. OSs typically permit system administrators to specify which types of events should be audited and whether successful and/or failed attempts to perform certain actions should be logged. OS logs might also contain information from security software and other applications running on the system.
- **Section Baseline security logging** – provides more information on application log data.
- Detailed responses to SOC’s security recommendations.

4. Records Management

All data and/or records generated during this procedure are stored in the NINDS SharePoint-based Document Library.

5. Review/Revision History

Date	Author/Reviewer	Description of Change
02/28/2019	Gladys Wang	Document Creation