# National Institutes of Health

# **OFFICE OF THE DIRECTOR (OD)**

# **NIH ETHICS OFFICE**

# **NIH ETHICS ENTERPRISE SYSTEM (NEES)**

# SYSTEM SECURITY PLAN (SSP)

# Draft

February 9, 2007

Prepared By Booz Allen Hamilton

#### SENSITIVE

Access to this information must be tightly restricted based on the concept of needto-know. Disclosure requires the approval of the owner of the information and, in the case of third parties, also a signed confidentiality agreement.

# TABLE OF CONTENTS

	<u>1</u>
1.1. SVCTEM NAME	1
1.2 System Categorization	1
1.3 RESPONSIBLE ORGANIZATIONS	1
1.4 INFORMATION CONTACTS.	1
1.4.1 Information System Owner	1
1.4.2 Authorizing Official	1
1.4.3 Other Designated Contacts	2
1.5 Assignment of Security Responsibility	2
1.6 System Operational Status	2
1.7 System Туре	3
1.8 General Description.	3
1.9 NEES Workflows	4
1.10 Users	10
1.11 System Environment	11
1.11.1 System Inventory	12
1.12 System Interconnection.	13
1.13 Applicable Laws, Regulation, and Policies Affecting the System	13
1.14 INFORMATION TYPE AND SECURITY CATEGORIZATION	15
1.14.1 Information Types or Information System Types	15
1.14.2 System Security Category	<u>16</u>
1.14.3 C&A Level of Effort (LOE) and Testing Formality	<u>19</u>
1.14.4 Types of Sensitive Information	<u>19</u>
1.15 Privacy Impact Assessment (PIA)	20
2 MANAGEMENT CONTROLS	21
2.1 Risk Assessment	<u>21</u>
2.1.1 Risk Assessment Policy and Policies	<u>22</u>
2.1.2 Security Categorization	22
2.1.3 Risk Assessment.	22
2.1.4 Risk Assessment Update	23
<u>2.1.5 Vulnerability Scanning</u>	23
<u>Z.Z PLANNING</u>	- 24
	24
2.2.1 Security Planning Policies and Procedures	24
2.2.1 Security Planning Policies and Procedures 2.2.2 System Security Plan	24
2.2.1 Security Planning Policies and Procedures 2.2.2 System Security Plan 2.2.3 System Security Plan Update	24 24 24 24
2.2.1 Security Planning Policies and Procedures 2.2.2 System Security Plan 2.2.3 System Security Plan Update 2.2.4 Rules of Behavior 2.2.5 Privacy Impact Assocsment	24 24 24 24 24
2.2.1 Security Planning Policies and Procedures 2.2.2 System Security Plan 2.2.3 System Security Plan Update 2.2.4 Rules of Behavior 2.2.5 Privacy Impact Assessment	24 24 24 24 24 26
2.2.1 Security Planning Policies and Procedures.         2.2.2 System Security Plan.         2.2.3 System Security Plan Update.         2.2.4 Rules of Behavior.         2.2.5 Privacy Impact Assessment.         2.3 System and Services Acquisition.         2.31 System and Services Acquisition.	24 24 24 24 26 26 26
2.2.1 Security Planning Policies and Procedures.         2.2.2 System Security Plan.         2.2.3 System Security Plan Update.         2.2.4 Rules of Behavior.         2.2.5 Privacy Impact Assessment.         2.3 System and Services Acquisition Policies and Procedures.         2.3.1 System and Services Acquisition Policies and Procedures.         2.3.2 Allocation of Resources	24 24 24 24 26 26 26 26
2.2.1 Security Planning Policies and Procedures.         2.2.2 System Security Plan.         2.2.3 System Security Plan Update.         2.2.4 Rules of Behavior.         2.2.5 Privacy Impact Assessment.         2.3 System and Services Acquisition Policies and Procedures.         2.3.1 System and Services Acquisition Policies and Procedures.         2.3.2 Allocation of Resources.         2.3.3 Life Cycle Support	24 24 24 24 26 26 26 26 26
2.2.1 Security Planning Policies and Procedures.         2.2.2 System Security Plan.         2.2.3 System Security Plan Update.         2.2.4 Rules of Behavior.         2.2.5 Privacy Impact Assessment.         2.3 System and Services Acquisition.         2.3.1 System and Services Acquisition Policies and Procedures.         2.3.2 Allocation of Resources.         2.3.3 Life Cycle Support.         2.3.4 Acquisitions	24 24 24 24 26 26 26 26 27 27
<ul> <li>2.2.1 Security Planning Policies and Procedures</li></ul>	24 24 24 26 26 26 26 26 27 27 27 27
<ul> <li>2.2.1 Security Planning Policies and Procedures</li></ul>	24 24 24 26 26 26 26 26 27 27 27 27 27 28
<ul> <li>2.2.1 Security Planning Policies and Procedures</li></ul>	24 24 24 26 26 26 26 26 27 27 27 27 27 27 28 28
<ul> <li>2.2.1 Security Planning Policies and Procedures</li></ul>	24 24 24 26 26 26 26 26 27 27 27 27 27 27 28 28 28 28
<ul> <li>2.2.1 Security Planning Policies and Procedures</li></ul>	24 24 24 26 26 26 26 26 26 27 27 27 27 27 27 28 28 28
<ul> <li>2.2.1 Security Planning Policies and Procedures.</li> <li>2.2.2 System Security Plan.</li> <li>2.2.3 System Security Plan Update.</li> <li>2.2.4 Rules of Behavior.</li> <li>2.2.5 Privacy Impact Assessment.</li> <li>2.3 System and Services Acquisition Policies and Procedures.</li> <li>2.3.1 System and Services Acquisition Policies and Procedures.</li> <li>2.3.2 Allocation of Resources.</li> <li>2.3.3 Life Cycle Support.</li> <li>2.3.4 Acquisitions.</li> <li>2.3.5 Information System Documentation.</li> <li>2.3.6 Software Usage Restrictions.</li> <li>2.3.7 User Installed Software.</li> <li>2.3.8 Outsourced Information System Services.</li> <li>2.3.10 Developer Configuration Management.</li> </ul>	24 24 24 26 26 26 26 26 27 27 27 27 27 28 28 28 28 28 28 28 28
<ul> <li>2.2.1 Security Planning Policies and Procedures.</li> <li>2.2.2 System Security Plan.</li> <li>2.2.3 System Security Plan Update.</li> <li>2.2.4 Rules of Behavior.</li> <li>2.2.5 Privacy Impact Assessment.</li> <li>2.3 System and Services Acquisition Policies and Procedures.</li> <li>2.3.1 System and Services Acquisition Policies and Procedures.</li> <li>2.3.2 Allocation of Resources.</li> <li>2.3.3 Life Cycle Support.</li> <li>2.3.4 Acquisitions.</li> <li>2.3.5 Information System Documentation.</li> <li>2.3.6 Software Usage Restrictions.</li> <li>2.3.7 User Installed Software.</li> <li>2.3.8 Outsourced Information System Services.</li> <li>2.3.9 Developer Configuration Management.</li> <li>2.3.10 Developer Security Testing.</li> </ul>	24 24 24 26 26 26 26 26 27 27 27 27 27 28 28 28 28 28 28 28 28 29 29
<ul> <li>2.2.1 Security Planning Policies and Procedures</li></ul>	24 24 24 26 26 26 26 26 26 27 27 27 27 27 27 27 27 27 28 28 28 28 29 29 30
<ul> <li>2.2.1 Security Planning Policies and Procedures</li></ul>	24 24 24 26 26 26 26 26 27 27 27 27 27 27 27 27 27 27 27 27 28 28 28 29 29 29 30 30

2.4.4 System Cortification	30
2.4.5 Plan of Action and Milostonos	<u></u>
2.4.5 Fiall of Action Accorditation	<u></u>
2.4.0 Security Accievitation	<u></u>
3. OPERATIONAL CONTROLS	<u>34</u>
3.1 DEDCONNEL SECURITY	34
3.1.1 Personnel Security Policies and Procedures	
3.1.2 Position Categorization	<u></u>
3.1.2 Personnel Screening	<u></u>
3.1.4 Personnel Termination	<u></u>
3.1.5 Personnel Transfer	37
3.1.6 Access Arreements	37
3.1.7 Third Party Personnel Security	37
3.1.8 Personnel Sanctions	37
3.2 Physical and Environmental Protection	37
3.2.1 Physical and Environmental Protection Policies and Procedures	38
3.2.2. Physical Access Authorization	39
3.2.3 Physical Access Control	39
3.2.4 Access Control for Access Medium	<u></u>
3.2.5 Access Control for Display Medium	<u></u>
3.2.6 Monitoring Physical Access	<u></u>
3.2.7 Visitor Control	<u>10</u> <u>/</u> 0
3.2.8 Access Logs	<u>40</u> 40
3.2.9 Power Equipment and Power Cabling	<u>10</u> 40
3.2.10 Fmergency Shutoff	<u>40</u> 40
3 2 11 Fmergency Power	<u>10</u> 40
3 2 1 2 Fmergency Lighting	<u>10</u> <u></u>
3.2.1.2 Fine Protection	41
3.2.14 Temperature and Humidity Controls	41
3.2.15 Water Damage Protection	41
3.2.16 Delivery and Removal	42
3.2.17 Alternate Work Site	42
3.3 CONTINGENCY PLANNING	42
3.3.1 Contingency Planning Policies and Procedures	4.3
3.3.2 Contingency Plan	4.3
3.3.3 Contingency Training	4.3
3.3.4 Contingency Plan Testing	4.3
3.3.5 Contingency Plan Undate	44
3.3.6 Alternate Storage Sites	
3.3.7 Alternate Processing Sites.	
3.3.8 Telecommunications Services.	
3.3.9 Information System Backup	
3.3.10 Information System Recovery and Reconstitution	
3.4 Configuration Management.	
3.4.1 Configuration Management Policies and Procedures	
3.4.2 Baseline Configuration	
3.4.3 Configuration Change Control	45
3.4.4 Monitoring Configuration Changes	
3.4.5 Access Restriction for Change.	
3.4.6 Configuration Settings	
3.4.7 Least Functionality	
3.5 Maintenance	
3.5.1 Maintenance Policies and Procedures	
3.5.2 Periodic Maintenance	

3.5.3 Maintenance Tools	47
3.5.4 Romoto Maintonanco	<u>4/</u> /7
3.5.5 Maintonanco Porconnol	<u>47</u> 18
3.5.6 Timoly Maintonanco	<u>40</u> 18
3.6 System and Internation Internation	<u>40</u> /18
3.6.1 System and Information Integrity Policies and Procedures	<u>40</u> /0
3.6.2 Elew Romodiation	<u>49</u> /0
3.6.3 Malicious Codo Protoction	<u>49</u> /0
3.6.4 Intrusion Dotoction Tools and Tochniques	<u>49</u> /0
2.6.5 Socurity Alorte and Advisories	<u>49</u> 50
3.6.6 Socurity Functionality and Vorification	<u>50</u> 50
3.6.7 Software and Information Integrity	<u>50</u> 50
3.6.8 Snam and Snuwara Protoction	50
3.6.9 Information Input Rostrictions	50
3.6.10 Information Input Accuracy Completeness and Validity	<u>50</u> 51
3.6.11 Fror Handling	51
3.6.12 Information Output Handling and Rotontion	<u>51</u> 51
3.7 MEDIA PROTECTION	<u>51</u> 51
2.7.1 Madia Protoction Policies and Procedures	<u>51</u> 52
3.7.2 Modia Accoss	<u></u>
3.7.2 Media Access	<u></u>
<u>3.7.4 Media Storago</u>	<u></u>
<u>3.7.4 Media Stolage</u> 3.7.5 Madia Transport	<u></u>
<u>3.7.6 Media Transport</u>	<u></u>
3.7.7 Media Destruction and Disposal	
2.9 INGEDENT DEGRONGE CADADUTE	<u></u>
2.9.1 Incident Response Capability Policies and Proceedures	
2.9.2 Incident Response Training	
2.9.2 Incident Response Trating	<u></u>
2.9.4 Incident Handling	<u>94</u> 54
2.9.5 Incident Monitoring	<u></u>
3.9.6 Incident Poporting	<u>55</u>
2.9.7 Incident Response Assistance	<u>55</u> 57
2.0. AWADENEESE AND TRADUNC	<u></u>
2.0.1 Awareness and Training Policies and Procedures	<u>57</u> 58
3.0.2 Socurity Awaronoss	<u>50</u> 58
3.0.3 Socurity Training	<u>50</u> 50
2.0.4 Socurity Training Pocorde	<u></u>
<u>5.5.4 Security framing Records</u>	
4. TECHNICAL CONTROLS	<u>59</u>
4.1 IDENTIFICATION AND ALTERITICATION	60
4.1 Identification and Authontication Policios and Procedures	<u></u> 60
4.1.1 Identification and Authoritication	<u>00</u> 60
4.1.2 Oser Identification and Authentication	<u>00</u> 61
<u>4.1.5 Device Identification and Admentication</u>	<u>01</u> 61
4.1.4 Identified Management	<u>01</u> 61
4.1.5 Authenticator Foodback	<u>01</u> 61
4.1.0 Automation recuback	<u>01</u> 61
4.1.7 Cryptographic Moune Authentication	<u>01</u> 61
A 2.1 Access Control Policy and Procedures	<u>01</u> 67
4.2.2 Account Management	<u>04</u> 62
4.2.3 Access Enforcement	<u>05</u> 62
1.2.1 Information Flow Enforcement	<u>05</u> 62
1.2.5 Separation of Duties	<u>05</u> 62
$\frac{1}{26}$ Jest Privilan	<u>05</u> 62
	05

4.2.7 Unsuccessful login attempts	64
4.2.8 System Use notification	64
4.2.9 Previous Logon Notification	<u>61</u> 64
4.2.10 Concurrent Session Control	
4.2.11 Session Lock	
4.2.12 Session Termination	64
4.2.13 Supervision and Review – Access Control	64
4.2.14 Permitted Actions w/o Identification or Authentication	64
4.2.15 Automated Marking.	65
4.2.16 Automated Labeling	
4.2.17 Remote Access	65
4.2.18 Wireless Access Restrictions.	
4.2.19 Access Control for Portable Mobile Systems	65
4.2.20 Personally Owned Information Systems	65
4.3 Audit and Accountability.	65
4.3.1 Audit and Accountability Policy and Procedures	66
4.3.2 Auditable Events	67
4.3.3 Content of Audit Records	67
4.3.4 Audit Storage Capacity	67
4.3.5 Audit Processing	67
4.3.6 Audit Monitoring, Analysis, and Reporting	67
4.3.7 Audit Reduction and Report Generation	67
4.3.8 Time Stamps	68
4.3.9 Protection of Audit Information.	68
4.3.10 Non-repudiation	68
4.3.11 Audit Retention.	68
4.4 Systems and Communication Protection.	68
4.4.1 System and Communications Protection Policy and Procedures	<u>69</u>
4.4.2 Application Partitioning	<u>69</u>
4.4.3 Security Function Isolation	<u>69</u>
4.4.4 Information Remnants	<u>69</u>
4.4.5 Denial of Service Protection	<u>69</u>
4.4.6 Resource Priority	<u>69</u>
4.4.7 Boundary Protection	<u>70</u>
4.4.8 Transmission Integrity	<u>70</u>
4.4.9 Transmission Confidentiality	<u>70</u>
4.4.10 Network Disconnect	<u>70</u>
4.4.11 Trusted Path	<u>70</u>
4.4.12 Cryptographic Key Establishment and Management	<u>70</u>
4.4.13 Use of Validated Cryptography	<u>70</u>
4.4.14 Public Access Protections	<u>70</u>
<u>4.4.15 Collaborative Computing</u>	<u>71</u>
<u>4.4.16 Transmission of Security Parameters</u>	<u>71</u>
<u>4.4.17 Public Key Infrastructure Certificates</u>	<u>71</u>
<u>4.4.18 Mobile Code</u>	<u>71</u>
<u>4.4.19 Voice Over Internet Protocol</u>	<u>71</u>
5. SYSTEM SECURITY PLAN STATEMENT OF APPROVAL	<u>72</u>
APPENDIX A - ACRONYMS	1
APPENDIX B - DOCUMENT HISTORY	1
APPENDIX C - SELF ASSESSMENT	1

APPENDIX D - SECURITY AND RISK ASSESSMENT REPORT1
APPENDIX E - PLAN OF ACTION AND MILESTONES1
APPENDIX F - ST& E PLAN AND PROCEDURES
APPENDIX G - RULES OF BEHAVIOR1
APPENDIX H - PRIVACY IMPACT ASSESSMENT1
APPENDIX I - CONTINGENCY PLAN1
APPENDIX J - CONFIGURATION MANAGEMENT PLAN1
APPENDIX K - ADDITIONAL SECURITY DOCUMENTATION1
LIST OF TABLES
TABLE 1: USER ROLES AND ASSIGNED PRIVILEGES10
TABLE 1: USER ROLES AND ASSIGNED PRIVILEGES
TABLE 1: USER ROLES AND ASSIGNED PRIVILEGES
TABLE 1: USER ROLES AND ASSIGNED PRIVILEGES
TABLE 1: USER ROLES AND ASSIGNED PRIVILEGES.10TABLE 2: SYSTEM INVENTORY.12TABLE 3: APPLICABLE LAWS, REGULATIONS, AND POLICIES.13TABLE 4: POTENTIAL IMPACT LEVELS.17TABLE 5: C&A LEVEL OF EFFORT.19
TABLE 1: USER ROLES AND ASSIGNED PRIVILEGES.10TABLE 2: SYSTEM INVENTORY.12TABLE 3: APPLICABLE LAWS, REGULATIONS, AND POLICIES.13TABLE 4: POTENTIAL IMPACT LEVELS.17TABLE 5: C&A LEVEL OF EFFORT.19TABLE 6: TYPES OF SENSITIVE INFORMATION WITHIN NEES.19
TABLE 1: USER ROLES AND ASSIGNED PRIVILEGES.10TABLE 2: SYSTEM INVENTORY.12TABLE 3: APPLICABLE LAWS, REGULATIONS, AND POLICIES.13TABLE 4: POTENTIAL IMPACT LEVELS.17TABLE 5: C&A LEVEL OF EFFORT.19TABLE 6: TYPES OF SENSITIVE INFORMATION WITHIN NEES.19LIST OF FIGURES19
TABLE 1: USER ROLES AND ASSIGNED PRIVILEGES.10TABLE 2: SYSTEM INVENTORY.12TABLE 3: APPLICABLE LAWS, REGULATIONS, AND POLICIES.13TABLE 4: POTENTIAL IMPACT LEVELS.17TABLE 5: C&A LEVEL OF EFFORT.19TABLE 6: TYPES OF SENSITIVE INFORMATION WITHIN NEES.19LIST OF FIGURES12FIGURE 1: NEES C&A BOUNDARY.4
TABLE 1: USER ROLES AND ASSIGNED PRIVILEGES.10TABLE 2: SYSTEM INVENTORY.12TABLE 3: APPLICABLE LAWS, REGULATIONS, AND POLICIES.13TABLE 4: POTENTIAL IMPACT LEVELS.17TABLE 5: C&A LEVEL OF EFFORT.19TABLE 6: TYPES OF SENSITIVE INFORMATION WITHIN NEES.19LIST OF FIGURES4
TABLE 1: USER ROLES AND ASSIGNED PRIVILEGES.10TABLE 2: SYSTEM INVENTORY.12TABLE 3: APPLICABLE LAWS, REGULATIONS, AND POLICIES.13TABLE 4: POTENTIAL IMPACT LEVELS.17TABLE 5: C&A LEVEL OF EFFORT.19TABLE 6: TYPES OF SENSITIVE INFORMATION WITHIN NEES.19LIST OF FIGURES19FIGURE 1: NEES C&A BOUNDARY.4FIGURE 2: NEES SECURITY CATEGORY FORMAT.18

# **1.SYSTEM IDENTIFICATION**

#### 1.1 SYSTEM NAME

The National Institute of Health (NIH) Ethics Enterprise System (NEES)

#### 1.2 SYSTEM CATEGORIZATION

LOW

MODERATE

HIGH

# **1.3 RESPONSIBLE ORGANIZATIONS**

Х

National Institutes of Health (NIH) Office of the Director (OD) NIH Ethics Office 2 Center Drive, Room BE21 Bethesda, MD 20892 Phone: (301) 594-9555

# 1.4 INFORMATION CONTACTS

# 1.4.1 Information System Owner

Sandra Desautels National Institutes of Health (NIH) Office of the Director (OD) Center for Information Technology (CIT) 6707 Democracy BLVD, Suite 307 Bethesda, MD 20817 <u>desautes@mail.nih.gov</u> Phone: (301) 402-6553

# **1.4.2 Authorizing Official**

Charlie H. Jones III Chief Information Officer (CIO) National Institutes of Health (NIH) Office of the Director (OD) Executive Office Building 6011 6011 Executive Boulevard, Room 214 Rockville, MD 20892 JonesC@od.nih.gov Phone: (301) 496-3973

# **1.4.3 Other Designated Contacts**

Holli Beckerman-Jaffe Information Owner Office of Ethics Office of the Director (OD) National Institutes of Health (NIH) 2 Center Drive, Room BE21 Bethesda, MD 20892 hj42q@.nih.gov Phone: (301) 594-9555

Dr. Steven Hausman User Representative National Institute of Arthritis and Musculoskeletal and Skin Diseases (NIAMS) 31 Center Drive, Room 4C 32E Bethesda, MD 20815 <u>hausmans@mail.nih.gov</u> Phone: (301) 402-1691

# 1.5 ASSIGNMENT OF SECURITY RESPONSIBILITY

Antoine Jones, Information Systems Security Officer (ISSO) National Institutes of Health (NIH) Office of the Director (OD) Office of Information Technology (OIT) 6011 Executive Boulevard, Suite 214 MSC 7652 Bethesda, MD 20892-7652 jonesa@od.nih.gov Phone: (301) 402-2949

# **1.6 SYSTEM OPERATIONAL STATUS**



The NEES information system is in the under development phase of its life cycle in accordance with the system development life cycle (SDLC) as defined in National Institute Standards of Technology (NIST) Special Publication (SP) 800-18.

#### **1.7 SYSTEM TYPE**

Х	Major Applicatio	General Support
	n	System

#### **1.8 GENERAL DESCRIPTION**

NEES is an Enterprise System that will migrate a previously manual process into an on-line process to include:

- The submission of all ethics-related reports and requests along with supporting documentation
- The review and approval process associated with these reports and requests
- The tracking of and reporting on all submissions, reviews, and approvals as well as other related activities that are associated with the Ethics Program at NIH

NEES version 1.0 has already been released, and includes the submission process for the Public Financial Disclosure Report (SF-278). The SF-278 is filed by all SES and SES-equivalent NIH employees as required by the Ethics in Government Act of 1978 and the Ethics Reform Act of 1989. Version 1.1 will embed tighter security controls which will be the baseline for future releases. The NEES system diagram is provided below in Figure 1.

Figure 1: NEES C&A Boundary

#### **1.9 NEES WORKFLOWS**

Below lists the NEES Process:

**1.** CIT controls the workflow from their custom code. The NEES system uses NIH SSO to authentication to IIS. The NEES system uses eFlow only as a pass-thru to two other servers/apps – Adobe Forms Server and Disk Xtender.

**2.** Once a form is completed, the Filer provide an electronic signature to the document and 'Submit' it by clicking a submit button.

**3.** Signed Ethics Forms will now enter the Reviewers Queues. Which Queue it enters is dependent on the IC, or job title of the Filer submitting the form. The Reviewer will have the form with the Dun & Bradstreet lookup, along with a comments section. If a Reviewer determines that a form does not

pass criteria, comments must be added to the comments section and the officer will click "Return to Filer". Or, if a form is complete the Reviewer will click "Complete". (See step 5)

**4.** If the Reviewer determines that the form needs to be returned to the user, an email is sent to the Filer notifying them that their ethics form needs to be modified. The Filer will then respond to the comments to clarify or explain.

**5.** If the Reviewer deems the Form complete it is submitted to the Certifier. The Certifier then conducts a secondary review and electronically signs the document. Then the PDF is updated, locked, and moved to the Documentum's ApplicationXtender for archiving and then exits the process.

**6.** Reports can be created from the NEES database and other appropriate databases.



NEES Process Map

Below are actual screen shots from the NEES application:

Login: Uses NIH Single Sign On then selects role.

•	🧝 💿 😭	Https://login.nih.gov/	siteminderagent/	orms/nihlogin.fcc: 📋 🔻	0(	G•	) <i>z</i> .
Getting Started	Latest Headlines 🔊	washingtonpost.com	Search Google	NIH Federal Credit U	NED	MapQuest	
		50					
	N	IIH Login					
	Us	er Name: NIHNEES					
	P	assword: *********		Change Password			
		Log in					

#### Warning Notice

This is a U.S. Government computer system, which may be accessed and used only for authorized Government business by authorized personnel. Unauthorized access or use of this computer system may subject violators to criminal, civil, and/or administrative action.

All information on this computer system may be intercepted, recorded, read, copied, and disclosed by and to authorized personnel for official purposes, including criminal investigations. Such information includes sensitive data encrypted to comply with confidentiality and privacy requirements. Access or use of this computer system by any person, whether authorized or unauthorized, constitutes consent to these terms. There is no right of privacy in this system.

Please e-mail questions or comments about NIH Login to nihhelpdesk@mail.nih.qov or call 301-594-6248.





# Main Menu for Filer Role:

MIH Enterprise I	Ethics System		D			ZENG, Jianping Filer Change Role   Log Out
	Re	epoi	rts List			
	Report	Type	Status	Actions		
	2006 New Entrant Report	SF 278	In Preparation	Edit Delete		
New Report If this is your first time using the NIH time using the "Instructions" link in t you'd like to report a bug or request	Enterprise Ethics System, ge he footer below. If you have a a change, use the Feedback Report	neral ins problem link. Type: [	tructions are avai or question, use	llable to help you get st the Contact Us link bel	arted. You can ow to locate th	view these at any e best resource. If

# Main Menu for Administrator Role:

NIH	Enterprise Ethics System		TE	ZENG, Jianping Administrator Change Role   Log Out
Employees				
Employee List	Personal Data			

# **Employee List**

Name, NIH ID, Ema				IC: File	r Status:	DEC: Senior Positio	n: Find I	mployee	
		Brows	e: <u>A B C D E F (</u>	эніл	<u>K L M N O P</u>		<u>uvwxyz</u>		
Results 1-8 of 8									
Name 🔺	<u>IC</u>	Organization	Postion Title	<u>Filer</u> <u>Status</u>	Role	Phone	<u>E-mail</u>	DEC Position	Senior Position (Top 5)
ANDERSON, Renitalynette K	СІТ	DNST	SUPVY ELEC ENGINEER	SF 278	Filer	301 594 9432	renita_anderson@nih.gov	No	No
GALLAGHER, Thomas J	СІТ	OD		SF 278	Filer	301 496 5703	tg149y@nih.gov	No	No
JONES, John F	СІТ	OD	COMPUTER ENGINEER	SF 278	Filer	301 496 5703	jonesjf@mail.nih.gov	No	Yes
MARTINO, Robert L	СІТ	DCB	SEN INVESTIGATOR (DIR DCB)	SF 278	Filer	301 496 1112	martino@mail.nih.gov	No	Yes
SCHMITZ, Helen M	СІТ	OD	IT SPECIALIST (SYSANALYSIS)	SF 278	Filer	301 496 2328	schmitzh@mail.nih.gov	No	No
SMALL, Jane M	СІТ	DCSS	SUPVY COMPUTER SCIENTIST	SF 278	Filer	301 435 2980	jane@mail.nih.gov	No	No
<u>WIMSATT, Kathryn</u> S	СІТ	EO	EXECUTIVE OFFICER	SF 278	Filer	301 496 0513	wimsatt@mail.nih.gov	No	No
ZENG, Jianping	СІТ	САВ		SF 278	Administrator, Assistant, Filer	301 402 6405	jz80i@nih.gov	No	No

Instructions | Security and Privacy Notice | Accessibility | Contact Us | Feed Back | Download Adobe Reader | NEES 1.0.2

Submenu: Section of the Preparation screens for Filers to report Assets:

My Info My Reports List Re	nterpris Reports aport Data	e Etl	nics Syst	<b>em</b> ents   Flags	s View	v/Print	TI		ZENG, Jianping Filer Change Role   Log Out
	SF 278, In Preparation – Jianping ZENG, 2006 New Entrant DUE DATE: 08/30/2006								
•	•	Q	<ul> <li><u>Do I have to report my personal</u> savings or checking accounts?</li> </ul>						
Getting Started Assets Other Income Liabilities Agreements Positions Compensations Wrap Up									<u>Are there any reporting</u> exceptions?
				Asset	S				<ul> <li><u>Do I need to attach a</u> <u>disqualification statement?</u></li> </ul>
Instructions: For y	ou, your spouse	e, and de	pendent children	, report each a	asset held	I for investment or	the produ	uction of income which	How do I view or print my <u>SF-278 report?</u>
had a fair market va reporting period, tog total more than \$5,0	alue exceeding s gether with such 000 (Note: This	\$1,000 at income. is a diffe	the close of the Report personal rent requirement	e reporting per savings and/ t than for the	lod, or wh or checkin OGE 450.	nich generated mor ng accounts in a sin .)	e than \$2 gle financ	00 in income during the cal institution if they	Why does my report say <u>"DRAFT"?</u>
Reporting Period:	From 1/1/200	5 throug	h your filing da	te. Value you	ır assets	as of any date y	ou choos	se that is less than 31	
days before your	ning date.								
Asset identifier	Type of	0	AccestMalue	Type of	Asset	C	Flores	A stilene	
	Asset	Owner	Asset value	Income	Incom	<u>e</u> <u>Comments</u>	Flags	Actions	
Bga Electronic Services	Checking or Savings Account	Self	\$500,001 - \$1,000,000	Interest	\$15,001 \$50,000		0	Edit Delete	
Federated Department Stores, Inc.	Stock, Bond, or Security	Joint	\$15,001 - \$50,000	Dividends	\$201 - \$1,000			Edit Delete	
International Business Machines Corporation	Stock, Bond, or Security	Self	\$1,001 - \$15,000	Interest Dividends	\$201 - \$1,000	۵		Edit Delete	
Microsoft Corporation	Stock, Bond, or Security	Self	\$15,001 - \$50,000					Edit Delete	
University of Maryland Baltimore County							0	Edit Delete	
Asset Attachmer	nts								
Name			Description			Туре		Actions	
Test	To test downlo	oad abili	ty			electronic		Download Delete	

# 1.10 USERS

NEES will support four different user roles, as shown in the following table:

Table 1: Us	er Roles and Assigned Privileges	

User Role	Available to:	<b>Description of Privileges</b>
Institutes and Centers	Respective IC	Can only search for, view, and
(IC) Administrator		maintain records for staff
		within their IC. Users can be
		assigned as administrators of
		more than one IC; however,
		they can only work within one

		IC at a time and must change roles to access records from another IC
National Institutes of Health (NIH) Administrator	NIH Ethics Office	Search, view and maintain records for all of NIH
Office of General Council (OGC) Administrator	HHS Office of General Council	Search and view records for all of NIH. Limited to only maintain records for a small subset of the NIH.
Filer	SES and SES-equivalent staff at NIH	Prepare, submit, and view their own SF-278 reports and can designate any NIH staff member as an assistant.
Assistant	NIH Staff	Prepare and view the SF-278 of the filer who has designated them.

Reviewers of the SF 278 form can be assigned at three levels. Each of these levels has two distinct roles; Reviewer and Certifier, with the certifier having the final signature authority:

- 1. IC Level See only SF 278 Filers within their institutes
- 2. NIH Level See and edit all Filers
- 3. Office of General Counsel (OGC) 2 person team who review executives, IC and NIH level reviewers, and certifiers (personnel who sign the form) activities.

Future roles and responsibilities will be added as future forms and/or functionalities are added to the system.

#### 1.11 SYSTEM ENVIRONMENT

NEES data will contain personnel financial information including assets, liabilities, financial transactions, and additional sensitive financial information that completes a full financial profile. Version 1.1 will incorporate SF 278 form which contains dollar asset information but in range form and will be publicly accessible within 60 days after submission. However, SES equivalent personnel within the Executive Branch of the office of the government, including the President and Vice-President of the United States are required to complete this form on an annual basis. In addition, future releases of the system will incorporate sensitive financial information that are not privy to the public however will not contain specific dollar amounts. Therefore, the system is considered sensitive due to the highest level of data sensitivity.

# 1.11.1System Inventory

#### Table 2: System Inventory

Component Name/ Server Name	Hardware Manufactur er (Name/Versi on)	Number	Software (Name/Versi on)	Locati on	Primary Function
NIHNEESSQL (SQL/ Record Manager)	HP Proliant BL40P Blade server	128.231.90. 35	MS SQL 2000	Bldg. 12 CR	SQL/Records Manager
NIHNEESWEB (IIS)	HP ProLiant BL20p server blade	128.231.90. 36	eFlow 2.0 Webclient, IIS 6.0	Bldg. 12 CR	Webserver
NIHNEESEFLOW (eFlow 3)	HP ProLiant BL20p server blade	128.231.90. 37	eFlow Services 2.0	Bldg. 12 CR	Workflow
NIHNEESAFSARX	HP ProLiant BL20p server blade	128.231.90. 39	Adobe Form Server	Bldg. 12 CR	Dynamic PDF generation
nihserchares (Adobe Reader Extension Server)	HP ProLiant BL20p server blade	128.231.90. 50	Adobe Intelligent Documents Platform	Bldg. 12 CR	Imaging server
nihserchads (Adobe Doc Server)	HP ProLiant BL20p server blade	128.231.90. 53	Adobe Document Server 6.0	Bldg. 12 CR	Adobe Extensions server
SAN	HP StorageWorks Enterprise Virtual Array 5000 200 GB	NIHSERCHD ISK is the front end for data storage for this project as NIHNEES SQL is for the databases	HP Storage Works	Bldg. 12 CR	Data and Image Storage
nihserchdisk	HP ProLiant BL20p server blade	128.231.90.4 7	Windows 2003 Server EMC Documentum DiskXtender 5.60	Bldg. 12 CR	SAN Management

# 1.12 SYSTEM INTERCONNECTION

NEES integrates with a number of other Enterprise Systems at NIH. NIH Employee Directory (NED) data is synced nightly; NEES syncs with HR Data Warehouse bi-weekly. The Integration Competency Center (ICC) in the Office of the Chief IT Architect will use the new Tibco product to create integrations with other systems at NIH -- nVision, Data Warehouse, NIDB, and ProTrak - and make this data available to NEES thru web services.

# 1.13 APPLICABLE LAWS, REGULATION, AND POLICIES AFFECTING THE SYSTEM

The following laws, regulations, and policies relevant to the NEES application are listed in Table 3.

Law, Regulation, Policy, or Standard	Relevance
Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources	Establishes a minimum set of controls to be included in Federal information technology (IT) security programs.
Computer Security Act of 1987	Sets the stage for protecting systems by codifying the requirement for Government- wide IT security planning and training.
Paperwork Reduction Act of 1995	Establishes a comprehensive information resources management framework including security and subsumed in the security responsibilities of the Computer Security Act of 1987.
Clinger-Cohen Act of 1996	Links security to agency capital planning and budget processes, establishes agency Chief Information Officers, and re-codifies the Computer Security Act of 1987.
Presidential Decision Directive (PDD) 63, "Protecting America's Critical Infrastructures"	Specifies agency responsibilities for protecting the nation's infrastructure, assessing vulnerabilities of public and private sectors, and eliminating vulnerabilities.
PDD 67, "Enduring Constitutional Government and Continuity of Government"	Relates to ensuring constitutional government, continuity of operations planning, and continuity of government operations.
OMB Memorandum 99-05, Instructions on Complying with President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records"	Instructs agencies on how to comply with the President's Memorandum of May 14, 1998, on "Privacy and Personal Information in Federal Records."

#### Table 3: Applicable Laws, Regulations, and Policies

Law, Regulation, Policy, or Standard	Relevance
OMB Memorandum 99-18, "Privacy Policies on Federal Web Sites"	Directs departments and agencies to post clear privacy policies on World Wide Web sites.
OMB Memorandum 00-13, "Privacy Policies and Data Collection on Federal Web Sites"	Is a reminder that each agency is required by law and policy to establish clear privacy policies for its Web activities and to comply with those policies.
General Accounting Office "Federal Information System Control Audit Manual"	Guides auditors in evaluating confidentiality, integrity, and availability controls of data maintained in computer systems.
National Institute of Standards and Technology (NIST) Special Publication (SP) 800-14, "Generally Accepted Principles and Practices for Security Information Technology Systems"	Guides organizations on the types of controls, objectives, and procedures that comprise an effective security program.
NIST SP 800-18, "Guide for Developing Security Plans for Information Technology Systems"	Details the specific controls that should be documented in a system security plan.
NIST 800-37, "Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems"	Details the process for conducting Certification and Accreditation activities for Federal Information Technology Systems.
NIST 800-53, "Recommend Security Controls for Federal Information Systems".	Guides organizations for selecting and specifying security controls for information systems supporting the executive agencies of the federal government. The guidelines apply to all components5 of an information system that process, store, or transmit federal information.
NIST 800-60, "Guide for Mapping Types of Information and Information Systems to Security Categories".	Assist Federal government agencies to categorize information and information systems.
Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems.	Contains legislative and executive mandates for improving the use and management of computers and IT systems in the Federal Government.
Health and Human Services (HHS) Information Security Program	Provides a baseline of security policies for HHS.
HHS, "Information Security Program Certification and Accreditation Guide"	Details the HHS tailored Certification and Accreditation process.
NIH Master IT Security Plan	Foundation document for the NIH Information Security Program. This document implements relevant federal laws, regulations, and policies that provide a basis for the information security policies for everyone at NIH.

Law, Regulation, Standard	Policy, or	Relevance
NIH Certification and Guidance	Accreditation	Provides an overview of the components of the NIH Certification and Accreditation (C&A) program as well as guidance on going through the C&A process.
NIH Certification and Policy	Accreditation	Ensures the confidentiality, integrity, and availability of NIH information through a risk-based and cost-effective approach to security. The policy will help ensure that system security safeguards are implemented correctly, effective in their application, and commensurate with the potential risks to the system and information.

#### 1.14 INFORMATION TYPE AND SECURITY CATEGORIZATION

As recommended in NIST SP 800-37 and in the FIPS 199 publications, the certification and accreditation (C&A) methodology employs security categorization to establish the required level of effort. This approach ensures that the appropriate level of effort is used to certify and accredit each system requiring a C&A. A system can be placed into one of three categories; High, Moderate, or Low. The level of documentation and testing necessary for the C&A process depends on the assigned category.

The methodology used in determining the security categorization and level of effort based on FIPS 199 is as follows for NEES:

- Identify Information Types or Information System Types;
- Select Provisional Impact Levels based on NIST SP 800-60, Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories, dated June 2004;
- Review and adjust based on client needs;
- Determine highest watermark for each security objective from all information types; and
- Assign System Security Category (SC) accordingly.

#### **1.14.1Information Types or Information System Types**

Based on NIST 800-60, "an information system may be a general support system (GSS), a major application (MA), or a local or special purpose system." The NEES system is considered a Moderate impact system (See section

<sup>&</sup>lt;sup>1</sup> NIST 800-60, Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories, June 2004.

1.4.1.3) and warrants it own security measures; therefore it is classified as a MA.

Following NIST SP 800-60 guidance, an information system can store, transmit and process several different types of information. Information types can be "mission-based" related to the "areas of operation" or "lines of business" associated with the purpose of an agency to conduct government operations. Appendix D of NIST SP 800-60, provides provisional impact levels as a recommended starting point for determining mission-based information types.

# 1.14.2System Security Category

The criteria used to determine the NEES SC (as defined in FIPS 199) are the potential impact on the organization or individuals should there be a breach of confidentiality, integrity, and availability of information stored, processed, and transmitted by the system. The terms are defined below and potential impact levels are shown in Table 3.

- *Confidentiality* is the prevention of intentional or unintentional disclosure of private or confidential information to unauthorized persons
- *Integrity* requirements ensure that information has not been changed accidentally or deliberately, and that it is accurate and complete
- *Availability* ensures the reliability of, and timely access to, data. System and information availability also assures that systems work promptly and service is not denied to authorized users.

	POTENTIAL IMPACT		
Security Objective	LOW	MODERATE	HIGH
<b>Confidentiality</b> Preserving authorized restrictions on information access and disclosure, including means for pro- tecting personal privacy and proprietary informa- tion. [44 U.S.C., SEC. 3542]	The unauthorized disclo- sure of information could be expected to have a <b>limited</b> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclo- sure of information could be expected to have a <b>serious</b> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclo- sure of information could be expected to have a <b>severe or catastrophic</b> adverse effect on organ- izational operations, or- ganizational assets, or individuals.
<i>Integrity</i> Guarding against improper information modification or destruction, and in- cludes ensuring informa- tion non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modifi- cation or destruction of information could be ex- pected to have a <b>limited</b> adverse effect on organ- izational operations, or- ganizational assets, or individuals.	The unauthorized modifi- cation or destruction of information could be ex- pected to have a <b>serious</b> adverse effect on organ- izational operations, or- ganizational assets, or individuals.	The unauthorized modifi- cation or destruction of information could be ex- pected to have a <b>severe or</b> <b>catastrophic</b> adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reli- able access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a <b>limited</b> adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a <b>serious</b> adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a <b>severe or catastrophic</b> adverse effect on organ- izational operations, or- ganizational assets, or individuals.

#### Table 4: Potential Impact Levels

Following NIST 800-60 guidance, an information system can store, transmit and process several different types of information. Information types can be "mission-based" related to the "areas of operation" or "lines of business" associated with the purpose of an agency to conduct government operations. Appendix D of NIST 800-60, provides provisional impact levels as a recommended starting point for determining mission-based information types.

NEES is a Government resources management system. Upon review of NIST SP 800-60, NEES stores, transmits, and processes information that closely maps to the *Reporting and Information Type*. Based on this type of data, the following impact levels are applicable for NEES:

SC Reporting and Information Type = (Confidentiality [Low]); (Integrity [Low]); (Availability [Low])

The highest level of data and information contained on the NEES is considered sensitive. The assigned impact levels for each security objective (confidentiality, integrity, and availability) for NEES are described below:

**Confidentiality:** Unauthorized disclosure will have a serious adverse effect on the NIH Ethics office. This may cause embarrassment to the agency. The confidentiality is ranked as **moderate**.

**Integrity**: Unauthorized modification will have a have a serious adverse effect on the NIH Ethic's office and individuals. Unauthorized modification to the financial data my result in incorrect data being submitted and reviewed which may lead to embarrassment of NIH and possible financial problems for the individual(s). The integrity is ranked as **moderate**.

**Availability**: The NEES Version 1.1. will contain the SF 278 form which requires that all filers must report and submit their forms by May 15<sup>th</sup> every year. Therefore the system must be available during that time. In addition, as additional forms are incorporated within NEES, additional deadlines will be added. However, if the system were not available, filers can submit paper copies to meet deadlines and/or the deadlines can be extended if the proper channels either internal or external to the system are followed. As such, if the system is unavailable this will cause a limited adverse effect to the NIH Ethics office during those critical times since there is an alternate process in submitting the forms. The availability is ranked as **low**.

In establishing the NEES SC, the highest watermark or maximum impact value for each security objective from the information types listed in Section 1.14.2 was analyzed using Table 4, Potential Impact Levels above. The categorization was adjusted based on the NEES system environment and in conversations with the NIH OD ISSO and the NEES system owner. Based on this analysis and the agreement amongst all applicable parties, the security category has been adjusted and the following is assigned for the NEES system (Figure 2).

#### SC <sub>NEES</sub> = (Confidentiality [Moderate]); (Integrity [Moderate]); (Availability [Low])

#### Figure 2: NEES Security Category Format

The NEES is therefore considered a moderate impact system, since the highest watermark of all security objectives is rated as **Moderate**.

# 1.14.3C&A Level of Effort (LOE) and Testing Formality

To determine the C&A LOE and testing formality of the system, the highest impact level from the security category was taken.

Table 5, *C&A Level of Effort*, lists the C&A activities required for Low, Moderate and High impact systems.

<b>Certification Impact</b>	rtification Impact Low (L)		High (H)
Certification LOE	Minimum	Detailed	Comprehensive
Documents	<ul> <li>Initial Risk Assessment</li> <li>System Security Plan (SSP)         <ul> <li>Contingency Plan</li> <li>Configuration</li> <li>Management Plan</li> <li>Incident Response Plan</li> <li>Security Awareness and Training Plan</li> <li>Rules of Behavior</li> <li>MOAs/ISAs</li> </ul> </li> <li>Risk Assessment Report</li> <li>Plan of Action and Milestones (POA&amp;M)</li> <li>C&amp;A Letters</li> </ul>	<ul> <li>Initial Risk Assessment</li> <li>System Security Plan (SSP)         <ul> <li>Contingency Plan</li> <li>Configuration</li> <li>Management Plan</li> <li>Incident Response Plan</li> <li>Security Awareness and Training Plan</li> <li>Rules of Behavior</li> <li>MOAs/ISAs</li> </ul> </li> <li>Security Assessment Report</li> <li>Plan of Action and Milestones (POA&amp;M)</li> <li>C&amp;A Letters</li> </ul>	<ul> <li>Initial Risk Assessment</li> <li>System Security Plan (SSP)         <ul> <li>Contingency Plan</li> <li>Configuration</li> <li>Management Plan</li> <li>Incident Response Plan</li> <li>Security Awareness and Training Plan</li> <li>Rules of Behavior</li> <li>MOAs/ISAs</li> </ul> </li> <li>Security Assessment Report</li> <li>Plan of Action and Milestones (POA&amp;M)</li> <li>C&amp;A Letters</li> </ul>
Certification Testing	<ul> <li>NIST SP 800-26</li> <li>GSS; Self-Assessment</li> <li>MA; Independent Assessment</li> <li>(No formal ST&amp;E required)</li> </ul>	<ul> <li>NIST SP 800-26 Self-Assessment</li> <li>Formal ST&amp;E</li> <li>Interviews &amp; Observations</li> <li>Minimal hands-on testing</li> <li>Vulnerability Scan (optional)</li> <li>Penetration Test (optional)</li> </ul>	<ul> <li>NIST SP 800-26 Self-Assessment</li> <li>Formal ST&amp;E</li> <li>Interviews &amp; Observations</li> <li>Complete hands-on testing</li> <li>Vulnerability Scan</li> <li>Penetration Test (optional)</li> </ul>

Since NEES is classified as a 'Moderate' impact system, the documents and certification testing activities listed under the '*Detailed*' column will be developed/updated and executed as part of the current C&A effort.

#### Table 5: C&A Level of Effort

#### **1.14.4Types of Sensitive Information**

This section describes the basic protection requirements for the NEES as determined by the sensitivity of the system and the data handled. The NEES application processes, stores and exchanges the following types of data, provided in Table 6 below:

#### Table 6: Types of Sensitive Information within NEES

	Patient Information
ü	Privacy Act
	Health/Physical Condition
ü	Confidential/Financial/Pro prietary
	Investigatory or Personnel

	Time Critical
	Diagnostic Information
	Clinical Center Trials
	Grants
	Contracts
	Research/Scientific Data
ü	Other

NEES data will contain personnel financial information including assets, liabilities, financial transactions, and additional sensitive financial information that completes a full financial profile. Version 1.1 will incorporate SF 278 form which contains dollar asset information but in range form and will be publicly accessible within 60 days after submission. However, SES equivalent personnel within the Executive Branch of the office of the government, including the President and Vice-President of the United States are required to complete this form on an annual basis. In addition, future releases of the system will incorporate sensitive financial information that are not privy to the public. Therefore, the system is considered sensitive due to the highest level of data sensitivity.

#### 1.15 PRIVACY IMPACT ASSESSMENT (PIA)

A PIA has not been conducted specifically for this system

#### 2.MANAGEMENT CONTROLS

This section describes the management control measures that are intended to meet the protection requirements of the NEES application. Management controls are security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security<sup>2</sup>. The types of control measures must be consistent with the need for protection of the system. According to NIST 800-53, the management controls class consists of the following families:

- Risk Assessment
- Planning
- System and Services Acquisition
- Certification, Accreditation and Security Assessments

#### 2.1 RISK ASSESSMENT

Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

There is an increasing trend towards developing "baseline" approaches to manage the risks of business computer applications. This concept proposes up front implementation of security controls for the most common and already recognized vulnerabilities of an operating environment. The process may eliminate the need to conduct extensive formalized quantitative risk analyses to cost justify protective measures that may be required.

This section, consisting of several parts, is designed and developed as a tool to collect general information about a business application/system and address the operating risk of a non-complex computer application-operating environment. It extracts the pertinent security related information from the instructions and directives to present a composite approach toward analyzing level of risk.

The methodology is intended to address the application and compliment the network information system security survey/accreditation. Final application accreditation assumes that the site information technology is accredited. A

<sup>&</sup>lt;sup>2</sup> National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*, February 2005.

self-assessment was conducted using the NIST SP 800-26 questionnaire titled *"Security Self Assessment Guide for Information Systems"*. The NIST self assessment is provided in Appendix C of this document.

Regardless of the protective measures in place, the key element to security in any computer environment is the user and how well the user follows established computer security policies and guidelines. It cannot be overemphasized that users are a major component in ensuring that the environment is as secure as necessary.

The Risk Assessment family consists of the following security controls:

- Risk Assessment Policy and Policies
- Security Categorization
- Risk Assessment
- Risk Assessment Update
- Vulnerability Scanning

#### 2.1.1 Risk Assessment Policy and Policies

See NIH Master IT Security Plan section 3.4, *Risk Management.* Risk assessments will be conducted every three years, or sooner if there are major changes to the operating platforms (i.e., Windows, UNIX, etc.). The Computer Information Technology Division of Computer Systems Services (DCSS) will conduct the risk assessments in accordance with NIST guidelines set forth in *NIST SP 800-30, Risk Management Guide for Information Technology Systems.* The basic procedure will be to gather a panel of knowledgeable staff to assess the vulnerabilities and threats (taking into consideration existing controls), and to make recommendations for additional controls. A three-by-three risk-level matrix will be used to assign risks. Management will make the final decision on the implementation of the recommended controls. Additionally, the risk assessment reports will be independently reviewed as part of the tri-annual certification process.

#### 2.1.2 Security Categorization

The security categorization for the NEES is moderate. This is documented in the NEES Certification and Accreditation Plan dated September 12, 2006, and in this System Security Plan (section 1.14.2).

#### 2.1.3 Risk Assessment

Currently the NEES is undergoing an assessment. This assessment will evaluate the managerial, operational and technical controls of the system. To date, no security audits have been done for NEES. This is because the application is still in the final stages of development. It is planned to be operational in December of 2006. A certification and accreditation (C&A) is currently in process and the system is undergoing its first assessment.

Since the system is considered 'moderate impact', a formal Security Test and Evaluation is required which would involve testing NIST 800-53 controls applicable for moderate impact systems only.

The self assessment will address control measures in place to mitigate potential exploits and identify measures that are needed to strengthen the security posture of the application.

The self assessment is located in Appendix C of this document followed by the latest Security and Risk Assessment report, POA&M, and ST&E Plan and Procedures in Appendix D, E, and F respectively.

# 2.1.4 Risk Assessment Update

In the future, risk assessments are planned for every 3 years, or if a major application change or upgrade occurs. These evaluations will document any new findings. Assessment documentation will be provided to the application manager and the OD/CIO. Based on this assessment, a corrective action plan or plan of action and milestones (POA&M) will be developed to address any findings.

# 2.1.5 Vulnerability Scanning

CIT performs a monthly scan of the servers on the OD network utilizing the Security Auditor's Research Assistant (SARA). The results of which are provided to the OD Security Group for resolution. SARA analyzes the network signature of a given host, assesses the signature for probable vulnerabilities, ranks the vulnerabilities in terms of severity, reports the vulnerabilities and suggests a remedial course of action.

The NEES system will undergo vulnerability scanning according to NIH Policy. OIT has performs periodic scans of the various components of the OIT LAN with a software package known as LANGuard Network Security Scanner. This software checks the network for possible security vulnerabilities by scanning the selected components of the network for missing security patches, services packs, open shares, open ports, unused user accounts, services/applications active on the computer, key registry entries, weak passwords, users and groups, and more.

OIT has purchased a scanning package known as WebInspect. This software scans web applications for compliance with enterprise policies and Health Insurance Portability and Accountability Act of 1996, Gramm-Leach-Bliley Act of 1999 and Sarbanes-Oxley regulations. The software includes a policy editor and templates, which list government requirements and check for proper access control, error handling, remote administration flaws, and other factors. The templates can flag vulnerabilities that would allow unauthorized access to backend databases. It can also suggest remediation steps, such as correcting ColdFusion error messages.

# 2.2 PLANNING

Organizations must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

The Federal Information Systems Management Act (FISMA) requires that all major applications and general support systems include the development and maintenance of a system security plan following NIST 800-18 guidance. Also, each system should have appropriate Rules of Behavior that all users must abide by for the system, and a Privacy Impact Assessment shall be conducted to determine the type and extent of personally identifiable information (PII, or Privacy Act data) contained within the system and how it is protected.

The Planning family consists of the following security controls:

- Security Planning Policies and Procedures
- System Security Plan
- System Security Plan Update
- Rules of Behavior
- Privacy Impact Assessment

# 2.2.1 Security Planning Policies and Procedures

See NIH Enterprise Master IT Security Plan section 3.10 System Security Plans.

# 2.2.2 System Security Plan

This is the first system security plan developed for NEES.

# 2.2.3 System Security Plan Update

The NEES system security plan is currently being developed for this C&A process. The plan will be reviewed once every three years or when significant changes occur to the system. The plan will be revised to address system/organizational changes or problems identified during plan implementation or security control assessments.

# 2.2.4 Rules of Behavior

Rules of Behavior are part of a comprehensive program to provide information security. The NIH Rules of Behavior establish standards of behavior in recognition of the following fact: knowledgeable users are the foundation of a successful security program. These rules extend to all NIH personnel and any other persons accessing NIH systems under formally established agreements. This includes contractors and other federally funded users. The NIH IT General Rules of Behavior can be found in appendix F of this document.

All users of the NIH network are expected to abide by all laws and regulations regarding the proper use of government information technology resources. Users are expected to comply with the following:

- The systems are to be used for official government business only. Users must not use the systems for personal gain, outside business activities, political activity, fund raising, charitable activity not sponsored by a government agency, or for playing games (even in learning situations).
- Users must not use systems to produce, store, display, or transmit material that is offensive to others including sexually explicit or suggestive materials.
   Users must not use the CIT systems to produce, store, display, or transmit material that constitutes harassment of other individuals on any basis including race, ethnicity, or sexual orientation.
- Users must not use the systems as a staging area for gaining unauthorized access to any other information systems or for, in any way, damaging, altering, or disrupting the operations of the other systems.
- Users must not use the systems and services for capturing or otherwise obtaining passwords, encryption keys, or any other access control mechanism that could permit unauthorized access to any computer system.
- Access to information on the systems is the sole responsibility of the "owner" - the account sponsor or registered user - of the information. Users must not access that information without the explicit permission of the owner, regardless of the degree of access control applied. The only exception is users may freely access information that is stored under a facility for general availability such as the World Wide Web or public libraries.
- Users are expected to use the services and facilities provided by the systems in accordance with the standards set forth in the appropriate guides.
- Users must not use electronic communications such as electronic mail to harass others, send obscene messages, forward chain letters or hoaxes, or send mass mailings indiscriminately.

Users who violate these Rules of Behavior are subject to disciplinary action in accordance with the NIH Information Technology General Rules of Behavior. These Rules of Behavior and other security policies and procedures are available to the user community through the CIT Computing Services Web page. All NEES users will be required to read and understand the NIH IT General Rules of Behavior.

# 2.2.5 Privacy Impact Assessment

See section 1.15 of this document.

# 2.3 SYSTEM AND SERVICES ACQUISITION

Organizations must: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect outsourced organizational information, applications, and/or services.

FISMA requires that organizations adequately plan for security throughout the lifecycle, that security be integrated into capital planning and programming and acquisition activities, and that all system acquisition activities comply with agency mandated use, documentation, and configuration management requirements.

The Systems and Services Acquisition family consist of the following security controls:

- Systems and Services Acquisition Policies and Procedures
- Allocation of Resources
- Life Cycle Support
- Acquisitions
- Information System Documentation
- Software Usage Restrictions
- User Installed Software
- Security Design Principles
- Outsourced Information Services
- Developer Configuration Management
- Developer Security Testing

# 2.3.1 System and Services Acquisition Policies and Procedures

See NIH Enterprise Master Security Plan Section 3.1 Acquisitions and<br/>Outsourced Operations and 3.2. System Life Cycle, NIH security policy NIH<br/>System Development Life Cycle (SDLC)<br/>IT Security Activities Matrix.

# 2.3.2 Allocation of Resources

NEES underwent an approval process which included security requirements. Resources are provided to adequately protect the system. The capital planning and investment control process is in its beginning stages at NIH, the NEES may be included in this process.

# 2.3.3 Life Cycle Support

Although a SSP can be developed for an application/system at any point in the life cycle, the recommended approach is to design the plan at the beginning of the system life cycle. It is recognized that in some cases, at any one time the application/system may be in several phases of the life cycle. For example, a large human resources system may be in the operation/maintenance phase, while an older, batch-oriented input sub-system is being replaced by a new, distributed, interactive user interface. In this case, the life cycle phases for the application/system include the disposal phase (data and equipment) related to the retirement of the batch-oriented transactions system, the initiation and acquisition phase associated with the replacement interactive input system, operations/maintenance phase for and the the balance of the application/system. Best practices suggest that planning for security should occur during each of the following life cycle phases:

- Initiation
- Development/Acquisition
- Implementation
- Operation/Maintenance
- Disposal.

The NEES information system is in the development/acquisition phase of its life cycle in accordance with the system development life cycle (SDLC) as defined in NIH Enterprise Master Security Plan Section 3.2 System Life Cycle, and the NIH security policy NIH System Development Life Cycle (SDLC) IT Security Activities Matrix.

# 2.3.4 Acquisitions

See NEES Deployment Document located in appendix K of this document, the Information Security Acquisition Provisions document, and the NIH Enterprise Master IT Security Plan, Sect. 3.1.

Security specifications for the NEES were referenced in the contractor's statement of work and based on an assessment of risk.

# 2.3.5 Information System Documentation

The NIH Ethics Office shall ensure that the following documentation is maintained and updated for NEES:

The following documentation is available for the NEES application:

- <u>**ü**</u> Requirements Analysis
- <u>**ü**</u> Design Specifications

- <u>**ü**</u> Independent Verification and Validation
- General Operating Procedures
- \_\_\_\_\_ User's Manual
- <u>ü</u> \_ Risk Assessment
- \_\_ Risk Management Plan
- <u>**ü**</u> Security Plan
- <u>**ü**</u> Contingency Plan
- \_\_\_\_ Disaster Recovery Plan
- <u>**ü**</u> Plan of Action and Milestones
- \_\_\_\_ Memorandum of Agreement/Understanding (N/A)
- <u><u><u><u>u</u></u> Vendor Documentation</u></u>
- <u><u><u><u>u</u></u> NIST Self Assessment</u></u>
- <u><u><u>u</u></u> Accreditation and Certification Letters</u>
- \_\_\_\_ Other (specify)

# 2.3.6 Software Usage Restrictions

**NIST Requirement:** The organization complies with software usage restrictions

The NEES will follow applicable NIH security policies and policies set forth in the NIH Master IT Security Plan. Use of software of unknown origin is not permitted.

# 2.3.7 User Installed Software

Users will be required to follow the NIH Policy on Limited Authorized Personal Use of NIH Information Technology (IT) Resources and the HHS-IRM-2000-0003, *HHS IRM Policy for Personal Use Of Information Technology Resources.* NEES users cannot download or install any unauthorized software.

# 2.3.8 Outsourced Information System Services

NMS provides web services which is integrated into the code and called when necessary.

# 2.3.9 Developer Configuration Management

Virtual Source Safe is used to manage the developer. The developer creates the installer for that release which is then put in the directory and a copy of the current configuration is put in repository. This is not a requirement for moderate impact systems.

# 2.3.10Developer Security Testing

This is part of internal testing before each release.

# 2.4 CERTIFICATION, ACCREDITATION AND SECURITY ASSESSMENTS

Organizations must: (i) periodically assess the security controls in organizational information systems to determine if the security controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the security controls.

FISMA requires that all federal major applications and general support systems be certified and accredited to operate. System security assessments should be conducted at least annually to determine the extent to which controls are implemented correctly, and operating as intended, while full C&As shall be conducted at least every 3 years or whenever significant system All information system interconnections outside the changes occur. boundary monitored accreditation shall be and approved through interconnection agreements. In addition, all relevant security deficiencies shall be tracked in a formal plan of actions and milestones (POA&M) and monitored continuously. Accreditation or authorization provides a form of quality control and is required under OMB Circular A-130, Appendix III. It forces managers and technical staff to find the best fit for security, given technical constraints, operational constraints, and mission requirements. By authorizing processing in a system, the DAA accepts the risk associated with operating the NEES information system.

The Certification, Accreditation and Security Assessments family consist of the following security controls:

- Certification, Accreditation, and Security Assessments Policies and Procedures
- Security Assessments
- Information System Connections
- System Certification
- Plan of Action and Milestones
- Security Accreditation
- Continuous Monitoring

#### 2.4.1 Certification, Accreditation, and Security Assessment Policies and Procedures

See NIH Enterprise Master Security Plan section 3.11 *Authorize Processing (Certification and Accreditation),* NIH *Certification and Accreditation Guidance* document and NIH *Certification and Accreditation Policy* document.

#### 2.4.2 Security Assessments

NIH C&A policy and guidance state that any system listed within the NIH System Inventory must undergo an annual security assessment following NIST 800-26. Therefore, the NEES will undergo an annual assessment.

#### 2.4.3 Information System Connections

NEES integrates with a number of other Enterprise Systems at NIH. NIH Employee Directory (NED) data is synced nightly; NEES syncs with HR Data Warehouse bi-weekly. The Integration Competency Center (ICC) in the Office of the Chief IT Architect will use the new Tibco product to create integrations with other systems at NIH -- nVision, Data Warehouse, NIDB, and ProTrak and make this data available to NEES thru web services.

All security forms needed to connect to these systems are completed. Transmission of information from NEES to these other systems and vice-versa is monitored by CIT and respective interconnected systems authorities. Please see **Appendix K** for these security forms.

# 2.4.4 System Certification

The NEES system is currently undergoing a C&A. The system is considered a moderate-impact system, therefore a formal ST&E is required. The ST&E will follow the NIST 800-53a which provides guidelines on how thoroughly to test the NIST 800-53 controls based on system impact level. The NEES was assessed against the moderate impact baseline controls only. Any findings will be incorporated into the POA&M and will be presented to the Certification Authority for review.

# 2.4.5 Plan of Action and Milestones

Based on the security risk assessment report which will provide detailed findings from the ST&E as well as recommendation, any findings will be incorporated into the POA&M. These include any security risks discovered through the C&A process that are to be addressed at a later date. The development and maintenance of the POA&M will follow the NIH POA&M Procedures guidance document. The POA&M will be reviewed and updated on a quarterly basis.
## 2.4.6 Security Accreditation

An Authority to Operate (ATO) authorizes use of a system by confirming that the system security plan is implemented adequately to secure the application. Results of the most recent review or audit of security controls shall be a factor in management's decision to grant authorization. The application must be authorized prior to operating and re-authorized at least every three years thereafter, unless there is a significant modification to system infrastructure that would change the overall security posture of the application. Management's authorization implies accepting the risk of the accredited application. The C&A participants at a minimum include the System Owner, DAA, and Certification Authority (CA). The responsibilities and contact information for those key personnel are provided in this section.

The NEES application is currently being assessed for accreditation. Booz Allen Hamilton is performing this certification and accreditation. The DAA, upon the recommendation from the Certification Authority, may authorize NEES for processing. If the NEES application meets the security requirements of HHS and NIH, the DAA should issue an ATO memorandum for the application.

## 2.4.6.1 INFORMATION SYSTEM OWNER

The Information System Owner represents the interests of the system throughout its life cycle (acquisition or maintenance, life cycle schedules, system operation, funding responsibility, system performance, and maintenance). The Information System Owner coordinates all aspects of the concept, svstem from initial development, implementation, system maintenance and disposal. The Information System Owner's function in the C&A process is to ensure that the security requirements are integrated in a way that will result in an acceptable level of risk to the operational infrastructure. The NEES Information System Owner is:

Sandra Desautels National Institutes of Health (NIH) Office of the Director (OD) Center for Information Technology (CIT) 6707 Democracy BLVD, Suite 307 Bethesda, MD 20817 <u>desautes@mail.nih.gov</u> Phone: (301) 402-6553

#### 2.4.6.2 DESIGNATED APPROVING AUTHORITY (DAA)/AUTHORIZING OFFICIAL

The DAA/Authorizing Official is an executive with the authority and ability to evaluate the mission, business case, and budgetary needs for the system in

view of the security risks. The DAA/Authorizing Official must have the authority to oversee the budget and business operations of IT systems under his/her purview. The DAA/Authorizing Official determines the acceptable level of residual risk for a system and establishes the approved system security posture.

The DAA/Authorizing Official is responsible for accepting a level of risk for the operation of the system and approving the system's security posture. Based on the information documented in the entire SSP, the DAA/Authorizing Official can grant an ATO, or may determine that the system's risks are not at an acceptable level and therefore the system is not ready to be operational. In reaching these decisions, the DAA is supported by all the documentation provided in the certification package. **The NEES DAA is:** 

Charlie H. Jones III Chief Information Officer (CIO) National Institutes of Health (NIH) Office of the Director (OD) Executive Office Building 6011 6011 Executive Boulevard, Room 214 Rockville, MD 20892 JonesC@od.nih.gov Phone: (301) 496-3973

#### 2.4.6.3 CERTIFICATION AUTHORITY (CA)

The CA provides the technical expertise to conduct the certification throughout the system's life cycle based on the system's security requirements. The CA determines the level of residual risk and makes an accreditation recommendation to the DAA.

The CA determines whether a system is ready for certification and conducts the certification process - a comprehensive evaluation of the technical and nontechnical security features of the system. At the completion of the certification effort, the certifier reports the status of certification and recommends to the DAA whether or not to accredit the system based on documented residual risk. The certifier should be independent from the organization responsible for system development or operation. Organizational independence of the certifier helps to ensure the most objective information is provided to the DAA for making accreditation decisions. **The NEES Certification Authority is:** 

Antoine Jones, Information Systems Security Officer (ISSO) National Institutes of Health (NIH) Office of the Director (OD) Office of Information Technology (OIT) 6011 Executive Boulevard, Suite 214 MSC 7652 Bethesda, MD 20892-7652 jonesa@od.nih.gov Phone: (301) 402-2949

#### 2.4.6.4 INFORMATION SYSTEMS SECURITY OFFICER (ISSO)

The principal staff advisor to the Information System Owner on all matters involving the security of the information system is the ISSO. The ISSO typically has the detailed knowledge and expertise required to manage the security aspects of the information system and, in many agencies, is assigned responsibility for the day-to-day security operations. The ISSO may be called upon to assist in the development of the system security policy and to ensure compliance with that policy on a routine basis. In close coordination with the Information System Owner, the ISSO often plays an active role in developing and updating the security plan for the information system as well as in managing and controlling changes to the system and assessing the security impact of those changes. **The NEES ISSO is:** 

Antoine Jones, Information Systems Security Officer (ISSO) National Institutes of Health (NIH) Office of the Director (OD) Office of Information Technology (OIT) 6011 Executive Boulevard, Suite 214 MSC 7652 Bethesda, MD 20892-7652 jonesa@od.nih.gov Phone: (301) 402-2949

#### 2.4.6.5 USER REPRESENTATIVE

The operational interests of Information System Owner and end-users are vested in the User Representative. In the C&A process, the User Representative is concerned with system availability, access, integrity, functionality, and performance in addition to confidentiality as they relate to the mission environment. System users are found at all levels of an agency. The users are responsible for the identification of operational requirements and the secure operation of a certified and accredited system, based on the approved security posture. The User Representative represents the Information System Owner and the user community through all phases of the system lifecycle. As such, the User Representative defines the system's operations and functional requirements while ensuring that the user's operational interests are maintained throughout system development, modification, integration, acquisition, and deployment. The NEES User **Representative is:** 

Dr. Steven Hausman User Representative National Institute of Arthritis and Musculoskeletal and Skin Diseases (NIAMS) 31 Center Drive, Room 4C 32E Bethesda, MD 20815 <u>hausmans@mail.nih.gov</u> Phone: (301) 402-1691

## 2.4.7 Continuous Monitoring

The POA&M will be reviewed on a quarterly basis, and a self assessment update will be conducted on a yearly basis. NEES will undergo a reaccreditation every three years or when a significant change occurs.

## **3.OPERATIONAL CONTROLS**

This section describes the operational control measures that are intended to meet the protection requirements of the system. Operational controls are security controls that are primarily implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise, and often rely upon management activities as well as technical controls. According to NIST 800-53, the operational controls class consist of the following families:

- Personnel Security
- Physical and Environmental Protection
- Contingency Planning
- Configuration Management
- Maintenance
- System and Information Integrity
- Media Protection
- Incident Response
- Awareness and Training

# 3.1 PERSONNEL SECURITY

Organizations must: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during personnel actions such as terminations and transfers; and (iii) employ

formal sanctions for personnel failing to comply with organizational security policies and procedures.

- HHS Instruction 731-1, *Personnel Security/Suitability Program*, policy states that:
  - (A) Every Department position, including those occupied by Commissioned Corps officers and those of contractors, must be designated with a sensitivity level. (Indian tribes and tribal organizations contracting under the Indian Self-Determination and Education Assistance Act are not considered contractors under this policy).
  - (B) All employees and contractors must meet personnel security/suitability standards commensurate with their position sensitivity level and they must be subject to personnel investigation requirements.
  - (C) Access to classified national security information is granted upon demonstration of a valid "need-to-know" and not merely on the basis of position, title, level of investigation conducted, or position sensitivity level.
  - (D) There is a reinvestigation requirement for individuals who have security clearances if they continue to have a need for access to classified information.

OMB Circular A-130, Appendix III calls for the periodic reinvestigation of information system privileged users. FISMA also requires that there be policies and procedures in place for handling all hiring, termination, and transfer activities for government staff, and that all third party staff abide by requirements set forth in agency personnel security rules.

The Personnel Security family consist of the following security controls:

- Personnel Security Policies and Procedures
- Position Categorization
- Personnel Termination
- Personnel Transfer
- Access Agreements
- Third-Party Personnel Security
- Personnel Sanctions

#### **3.1.1 Personnel Security Policies and Procedures**

\_X\_ In Place \_\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

See HHS Instruction 731-1, *Personnel Security/Suitability Program* and the NIH Enterprise Master Security Plan Section 4.1.1, *Background Investigations*.

#### 3.1.2 Position Categorization

## \_X\_ In Place\_\_ Planned\_\_ In Place & Planned\_\_ Not Applicable

At the NIH level, all positions with direct access to the system have been reviewed for sensitivity and individuals have been or will be subject to background checks appropriate to the position to which they are assigned.

NIH has documented personnel policies and procedures covering all critical aspects of employment services. The consolidated NIH Human Resources (HR) department is responsible for all procedures relevant to hiring and screening practices. The Office of Research Services in the Office of the Director, is the organization where NIH HR is located. DCSS has classified employees according to sensitivity levels and as of August, 2004, HR began the process of having appropriate background investigations conducted.

All new employees are classified according to sensitivity levels and receive an employee information kit explaining various procedural and administrative matters applicable to them. New hires are granted access to appropriate systems according to their job functions prior to completion of their background investigations. See HHS Instruction 731-1, *Personnel Security/Suitability Program* for further detail.

#### **3.1.3 Personnel Screening**

## \_X\_ In Place\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

At the NIH level, all positions with direct access to the system have been reviewed for sensitivity and individuals have been or will be subject to background checks appropriate to the position to which they are assigned. External users, which are considered the general public of the system are only subject to acknowledging and signing information within the log in screen.

The consolidated NIH Human Resources (HR) department is responsible for all procedures relevant to hiring and screening practices.

#### **3.1.4 Personnel Termination**

# \_X\_ In Place\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

System Administrators will terminate a users account by inactivating the user's record within the NEES "account" table. For security and data continuity reasons, person record deletions are not permitted. User accounts may be terminated/inactivated if the person leaves an institution, changes jobs within the institution, or has not used NEES for 180 days. Users within NIH will have their accounts deactivated if they cease to be employed within NIH Ethics Office/NIH.

Upon termination of employment, employees and contractors are required to return all ID badges, keys, and CIT-issued equipment. The departed employee's/contractor's accounts on all systems are deactivated. HR sends a checklist to the departing employee's/contractor's manager to ensure these actions are completed. These procedures are followed for both friendly and unfriendly terminations. The NEES system will follow the termination procedures set forth by NIH.

## **3.1.5 Personnel Transfer**

## \_X\_ In Place\_\_\_ Planned\_\_ In Place & Planned\_\_ Not Applicable

If an NIH user moves to another department within NIH, he or she will have their account reviewed for either inactivation or modification of user role. A note is sent to the help desk to deactivate account and take back FOB, parking garage pass and facility pass. The NEES will follow transfer procedures set forth by NIH.

#### **3.1.6 Access Agreements**

## \_X\_ In Place \_\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

All NIH employees are required sign a rules of behavior, non disclosure agreement, <u>NIH Remote Access User Certification Agreement</u>, and any additional access agreements for personnel requiring access to organizational information and NEES before authorizing access.

# 3.1.7 Third Party Personnel Security \_X\_ In Place \_ Planned\_\_ In Place & Planned\_\_ Not Applicable

Third party vendors and contractors are subject of the same investigative and personnel security requirements as NIH employees. See HHS Instruction 731-1, *Personnel Security/Suitability Program* for further detail.

#### **3.1.8 Personnel Sanctions**

## \_X\_ In Place \_\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

NIH HR processes govern enforcement of sanctions on government staff. NIH employees take the NIH security awareness course online as an annual refresher on security. Accounts are automatically disabled for those NIH users who fail to take the online course.

#### 3.2 PHYSICAL AND ENVIRONMENTAL PROTECTION

Organizations must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for

information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

The NIH Master Security Plan requires that NIH ensure that rooms, work areas/spaces, and facilities that contain NIH IT resources that process, transmit, or store sensitive or privacy information implement physical protection measures that are commensurate with the level of risk. In addition, FISMA requires that all data processing facilities have monitored access, that visitors always be authenticated and monitored, and that the facilities have adequate power, HVAC, emergency lighting, emergency shutoff, fire protection, temperature and humidity control, and water damage protection. Also, delivery and removal of equipment and resources from controlled areas should be strictly controlled.

Physical and environmental security controls protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation.

The Physical and Environmental Protections family consist of the following security controls:

- Physical and Environmental Protections Policies and Procedures
- Physical Access Authorization
- Physical Access Control
- Access Control for Access Medium
- Access Control for Display Medium
- Visitor Control
- Access Logs
- Power Equipment and Power Cabling
- Emergency Shutoff
- Emergency Power
- Emergency Lighting
- Fire Protection
- Temperature and Humidity Controls
- Water Damage Protection
- Delivery and Removal
- Alternate Work Site

## **1** Physical and Environmental Protection Policies and Procedures

\_X\_ In Place \_\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

See NIH Master Security Plan Section 4.2, *Physical and Environmental Protection* and Section 4.3, *Environmental Security*. All physical controls will be handled by CIT.

## 3.2.2 Physical Access Authorization

# \_X\_ In Place \_\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

The NEES application and database will be hosted on a web server and database server located in Building 12. Building 12 is located at 12 South Drive in Bethesda MD. A data key, to which only system administrators have access, protect this room.

At the end of each calendar year, the list of individuals authorized data center access is reviewed and managers confirm continued need for access.

# 3.2.3 Physical Access Control

\_X\_ In Place \_\_\_\_ Planned \_\_\_ In Place & Planned\_\_\_ Not Applicable

The room housing the NEES Development Server is within a facility that allows limited access with both physical keys (suite access) and security swipe keys (building access) and is monitored 24 hours a day. Below describes the physical access controls in place at building 12.

Access to all building on the NIH Campus is controlled via security guards at authorized entrances or via a badge reader. Only those personnel with NIH issued access cards are allowed entry to the buildings on campus without signing in. All other personnel entering the building must present proper identification and a temporary (sticker) badge is issued to the person. This temporary badge will also allow access to other buildings. NetBotz have been installed in all of the various computer rooms under OD control. These devices provide the ability to monitor temperature, presence of water, and provide a video capture of the door when it is opened along with other monitoring capabilities. Access to Room 3B33 requires a physical key if the there are no OIT staff members in present. Additionally, access to the computer room within the suite is controlled by a separate locked door and contains a window allowing visual access. The walls, doors, and windows of the computer room within Room 3B33 are designed, constructed, and installed to minimize the possibility of unauthorized access. There are locks on terminals and server racks.

## 3.2.4 Access Control for Access Medium

\_X\_ In Place \_\_\_\_ Planned\_\_\_ In Place & Planned \_\_X\_\_ Not Applicable

Not required for any of the security baselines; CIT controls the data transmission lines and their access.

# 3.2.5 Access Control for Display Medium \_X\_ In Place \_\_\_\_\_ Planned\_\_\_\_ In Place & Planned \_\_\_\_\_ Not Applicable

Handled by CIT.

## **3.2.6 Monitoring Physical Access**

```
___ In Place ____ Planned___ In Place & Planned___ Not Applicable
```

See section 3.2.3 of this document.

## 3.2.7 Visitor Control

# \_X\_ In Place \_\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

Individuals, such as equipment repair persons, are required to complete a visitor log and must be escorted to the computer room. Visitors must display an "Escort Required" badge and be accompanied by a person authorized for unescorted access to the computer room.

#### 3.2.8 Access Logs

# \_X\_ In Place \_\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

All visitors are required to sign a visitor's log. The visitor log contains name and agency of the person visiting; signature of the visitor; form of identification; date of access; time of entry and departure; purpose of visit; and name and NIH of person visited.

# 3.2.9 Power Equipment and Power Cabling \_\_X\_\_ In Place \_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

Handled by CIT.

# **3.2.10Emergency Shutoff**

## \_X\_ In Place \_\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

The data center equipment is protected from power surges, drops, or interruptions by an Uninterruptible Power Supply (UPS) system. The UPS system is designed to provide all electrical services to the data center area. When an interruption occurs, power is supplied by a battery backup system having up to 30 minutes of operating capability. Beyond 30 minutes, diesel generators provide more than 24 hours of operation per tank of fuel. The UPS system has more than 50% excess capacity. Moreover, the batteries, monitoring and control equipment, and diesel generators all are configured in three redundant sections. Failure of any one section will result in no more than a one-third loss of capability, leaving more than adequate capacity to support all ongoing services until power is restored.

## **3.2.11Emergency Power**

\_X\_ In Place \_\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

Servers will be protected against power outages and spikes by an uninterrupted power supply (UPS). When an interruption occurs, power is supplied by a battery backup system having up to 30 minutes of operating capability. Beyond 30 minutes, diesel generators provide more than 24 hours of operation per tank of fuel.

#### **3.2.12Emergency Lighting**

\_X\_ In Place \_\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

Handled by CIT.

#### **3.2.13Fire Protection**

\_X\_ In Place\_\_\_ Planned\_\_ In Place & Planned\_\_ Not Applicable

All rooms contain equipment and have policies in place that are designed to facilitate fire prevention, fire protection, and fire suppression. These may include: prohibition of smoking; keeping room free of trash; smoke or fire detectors which are connected to a central guard station; H2O sprinkler system; CO2 extinguishers; or type ABC fire extinguishers. Specifications are as regulated by county or state building codes for the type of commercial facility, and is the responsibility of the building management.

The machine room is equipped with smoke detectors and an adequate number of fire extinguishers to contain small fires. The NIH fire department on campus can respond to an alarm within minutes. Air cooling of the machine room is supplied by the NIH campus-wide chilled water system. There are backup pumps for chilled water distribution in the data center and the UPS will run the chilled water pumps in the event of extended power outage. The chilled water pipes run along the ceiling of the first floor area and under the floor of the second floor area.

# 3.2.14Temperature and Humidity Controls \_X\_ In Place \_\_\_ Planned \_\_ In Place & Planned \_\_ Not Applicable

Air cooling of the machine room is supplied by the NIH campus-wide chilled water system. There are backup pumps for chilled water distribution in the data center and the UPS will run the chilled water pumps in the event of extended power outage. The chilled water pipes run along the ceiling of the first floor area and under the floor of the second floor area. Also there are two free standing supplementary air cooling units.

## **3.2.15Water Damage Protection**

\_X\_ In Place \_\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_\_ Not Applicable

Drop cloths are kept in the data center to cover affected equipment should a leak occur. NIH maintenance is on call and available 24x7 to make emergency repairs for plumbing leaks and chilled water distribution.

#### 3.2.16 Delivery and Removal

## \_X\_ In Place\_\_ Planned\_\_ In Place & Planned\_\_ Not Applicable

For removal of equipment, each piece of equipment has its own individual inventory control sticker. Personnel who are removing equipment must possess a property pass that documents the date of removal, serial number of equipment and destination. For equipment delivery, all equipment must go to the building depot and undergo the package receiving process.

## 3.2.17Alternate Work Site

## \_X\_ In Place\_\_ Planned\_\_ In Place & Planned\_\_ Not Applicable

Handled by CIT.

#### 3.3 CONTINGENCY PLANNING

Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

A security contingency is an event with the potential to disrupt operations, thereby disrupting mission critical functions. Such an event could be a power outage, hardware or software failure, software compromise (e.g., from malicious hacking, viruses, or worms), fire, or storm. Contingency planning and procedures are required to provide reasonable assurance that critical data processing support can be sustained or quickly restored if normal system operations are interrupted. The NEES contingency plan is located in Appendix H of this document.

The Contingency Planning family consist of the following security controls:

- Contingency Planning Policies and Procedures
- Contingency Plan
- Contingency Training
- Contingency Plan Testing
- Contingency Plan Update
- Alternate Storage Sites
- Alternate Processing Sites
- Telecommunications Services

- Information System Backup
- Information System Recovery and Reconstitution

# 3.3.1 Contingency Planning Policies and Procedures

\_X\_ In Place \_\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

See NIH Master Security Plan Section 4.9, *Contingency Planning*, NIH IT Contingency Planning Policy, and HHS *Contingency Planning for Information Security Guide.* 

#### **3.3.2 Contingency Plan**

\_\_\_ In Place \_\_\_\_ Planned \_\_X\_ In Place & Planned \_\_\_ Not Applicable

NIH requires that all contingency plans should:

- identify contingency roles, responsibilities, individuals with contact information, and activities associated with restoring the system after a disruption or failure.
- be tested to determine their effectiveness and the organization's readiness to execute the plan.
- be reviewed and revised to address system/organizational changes or problems encountered during plan implementation, execution, or testing.
- identify alternate storage sites and initiate necessary agreements to permit the storage of information system backup information.
- identify alternate processing sites and initiate necessary agreements to permit the resumption of information system operations for critical mission/business functions when the primary processing capabilities are unavailable.
- employ mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to the system's original state after a disruption or failure.

See the NEES IT contingency plan in Appendix H of this document.

## **3.3.3 Contingency Training**

\_\_\_ In Place \_\_\_ Planned \_\_X\_ In Place & Planned \_\_\_ Not Applicable

Training should occur at least annually.

#### **3.3.4 Contingency Plan Testing**

\_\_\_ In Place \_\_\_ Planned \_\_X\_ In Place & Planned \_\_\_ Not Applicable

Testing should occur at least annually.

## **3.3.5 Contingency Plan Update**

```
___ In Place ____ Planned __X_ In Place & Planned ___ Not Applicable
```

The plan should be reviewed at least annually.

# 3.3.6 Alternate Storage Sites \_\_\_\_\_ In Place \_\_\_\_\_ Planned\_\_\_\_ In Place & Planned \_X\_ Not Applicable

No Alternate Storage Site in place.

## 3.3.7 Alternate Processing Sites

\_\_\_ In Place \_\_\_\_ Planned\_\_\_ In Place & Planned \_\_\_ Not Applicable

Alternate processing sites not in place.

#### 3.3.8 Telecommunications Services

\_\_\_ In Place \_\_\_ Planned\_\_\_ In Place & Planned \_\_\_\_ Not Applicable

Telecommunications service is not in place.

## 3.3.9 Information System Backup

# \_X\_ In Place \_\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

The NEES SQL databases will be backed up nightly to a tape library. Four weeks of tapes will be retained. The NEES Web Server hard disks will be backed up weekly. Four weeks of hard disk content backups will be retained. Any back up materials will be stored off-site in Building 2.

Backups are not tested due to the nature of the data.

# 3.3.10Information System Recovery and Reconstitution \_X\_ In Place \_\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

Procedures for recovering from short-term outages due to hardware/software failures will be in place and documented in the contingency plan.

The Project Officer will be responsible for coordinating hardware replacement, should the development server fail. CIT maintains a comprehensive spare parts inventory in addition to having complete spare servers available. CIT should have a server replacement on-line within one business day. Users will be notified that interruption in availability will not exceed this length of time.

#### 3.4 CONFIGURATION MANAGEMENT

Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems; (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems; and (iii) monitor and control changes to the baseline configurations and to the constituent components of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles

The NIH Master Security Plan requires that NIH establish, implement, and enforce change management and configuration management controls on all NIH systems and networks that process, store, or communicate sensitive information, to include the preparation of configuration control plans for all NIH systems and networks.

The Configuration Management family consist of the following security controls:

- Configuration Management Policies and Procedures
- Baseline Configuration Plan
- Configuration Change Control
- Monitoring Configuration Changes
- Access Restriction for Change
- Configuration Settings
- Least Functionality

## 3.4.1 Configuration Management Policies and Procedures

\_X\_ In Place \_\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

See NIH Master Security Plan Section 3.3, *Change Management Control* and the NIH *Configuration Management Plan* template. A separate configuration plan for NEES will be developed by the end of this C&A.

#### **3.4.2 Baseline Configuration**

\_X\_ In Place \_\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

A NEES Deployment Plan is in place for NEES.

## **3.4.3 Configuration Change Control**

\_X\_ In Place \_\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

Handled by CIT.

## 3.4.4 Monitoring Configuration Changes

\_X\_ In Place \_\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

Handled by CIT.

## 3.4.5 Access Restriction for Change

\_X\_ In Place \_\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

See section 3.4.3.

## **3.4.6 Configuration Settings**

\_X\_ In Place \_\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

See technical controls section of this document for further detail.

## **3.4.7 Least Functionality**

\_X\_ In Place \_\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

Handled by CIT.

## 3.5 MAINTENANCE

Organizations must: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

Based on the NIH Master Security Plan all NIH hardware and software should be tested, documented, and approved prior to promotion to production and that only authorized personnel conduct maintenance on all NIH hardware and software.

The Maintenance family consist of the following security controls:

- Maintenance Policies and Procedures
- Periodic Maintenance
- Maintenance Tools
- Remote Maintenance
- Maintenance Personnel
- Timely Maintenance

## 3.5.1 Maintenance Policies and Procedures

\_\_X\_ In Place \_\_\_\_ Planned\_\_\_ In Place & Planned\_X\_\_ Not Applicable

See NIH Master Security Plan Section 4.8.6, *Hardware/Software Maintenance*.

#### **3.5.2 Periodic Maintenance**

## \_X\_ In Place \_\_\_\_ Planned\_\_ In Place & Planned\_ \_\_ Not Applicable

Hardware maintenance controls are used to monitor the installation of, and updates to hardware to ensure that the hardware functions as expected and that a historical record of changes is maintained. Software maintenance controls are used to monitor the installation of, and updates to, operating system software, application software, and other software to ensure that the hardware and software function as expected and that a historical record of changes is maintained.

The CIT Desktop team is responsible for making sure the customer's desktop equipment functions properly. Support may involve working with members of other teams such as the Infrastructure team, the Server team, and the Applications team. The NIH Help Desk is used for receiving problem reports during and after normal business hours. Additionally, blackberries and cell phones are available to everyone at CIT. These devices provide the CIT staff with instant notification when an emergency is reported.

Repairs are done in house. When a piece of hardware malfunctions, the CIT staff assesses the problem, orders replacement parts from the manufacturer if necessary, and repairs the equipment.

In order to protect the audit logs from unauthorized misuse, there are tight controls over the access to the servers. There is a separate domain that CIT uses to test service packs and changes prior to implementation of the modification in the production environment. CIT conducts an impact analysis prior to making system changes on an ad-hoc basis. All system maintenance is conducted periodically.

CIT has NIH property stickers on all NIH owned equipment. An NIH property custodian must follow documented NIH property management procedures to track the location of equipment. CIT does not allow remote diagnostics and maintenance services on their hardware. There is a three (3) year warranty for servers. Server maintenance (security updates and patches) is performed every third weekend of the month. Emergency patches are performed when released. All maintenance logs are maintained by CIT.

## 3.5.3 Maintenance Tools

\_X\_ In Place \_\_ Planned\_\_ In Place & Planned\_\_ Not Applicable

Handled by CIT.

## 3.5.4 Remote Maintenance

\_X\_ In Place \_\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

System administrators will have the ability to perform their duties from a remote location. Remote access is monitored by CIT.

## **3.5.5 Maintenance Personnel**

## \_X\_ In Place \_\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

See sections 3.2.7 and 3.5.2. Handled by CIT.

## **3.5.6 Timely Maintenance**

## \_X\_ In Place\_\_ Planned\_\_ In Place & Planned\_\_ Not Applicable

Handled by CIT.

## 3.6 SYSTEM AND INFORMATION INTEGRITY

Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

System and Information integrity controls are intended to protect data from accidental or malicious alteration or destruction and to provide assurance to the user that the information has not been altered. Validation controls refer to tests and evaluations used to determine compliance with security specifications and requirements. Based on NIH appropriate NIH systems and networks should be equipped with data integrity and validation controls to provide assurance that NIH information has not been altered or deleted

The System and Information Integrity family consist of the following security controls:

- System and Information Integrity Policies and Procedures
- Flaw Remediation
- Malicious Code Protection
- Intrusion Detection Tools and Techniques
- Security Alerts and Advisories
- Security Functionality and Verification
- Software and Information Integrity
- Spam and Spyware Protection
- Information Input Restrictions
- Information Input Accuracy, Completeness, and Validity
- Error Handling
- Information Output Handling and Retention

# 3.6.1 System and Information Integrity Policies and Procedures

# \_X\_ In Place \_\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

Integrity controls are used to protect the operating system, applications, and information in the system (including data) from accidental or malicious alteration or destruction and to provide assurance to the user that the information meets expectations about its quality and that it has not been altered. See NIH Master Security Plan Section 4.5 *Data Integrity*, NIH *Patch Management Policy* and *Patch Management Guidance* documents and the NIH *Automatic Antivirus Policy* document.

#### 3.6.2 Flaw Remediation

# \_X\_ In Place \_\_\_\_ Planned\_\_\_ In Place & Planned\_ \_\_ Not Applicable

NIH requires the following for patch management:

- 1. Critical security patches must be kept up-to-date on all systems connected to NIHnet. Automatic loading of patches should be employed whenever feasible.
- 2. Automatic loading of patches is required on commodity desktops. For critical vulnerabilities that require immediate action, remotely rebooting commodity desktops is required.
- 3. Reporting of patch status will be made to the NIH Incident Response Team in a frequency and format determined by the NIH CISO.

Please refer to the '*NIH Patch Management Guidance*' document for further details.

Software patches and upgrades to the Operating System and Database Server software are installed by CIT once the new software updates have been deemed necessary and stable. Stability is determined by installation on a test server or on a similar server as determined by the CIT Staff. Patches are installed every third Saturday of the month.

## 3.6.3 Malicious Code Protection

# \_X\_ In Place\_\_\_\_ Planned\_\_ In Place & Planned\_ Not Applicable

Antivirus software will be installed on the servers NEES software will be placed on. This software will be configured to automatically scan newly loaded software and periodically update virus definitions.

#### **3.6.4 Intrusion Detection Tools and Techniques**

\_X\_ In Place \_\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

Intrusion detection is handled at the network level firewalls and is the responsibility of the NIH Incident Response Team (IRT) which is in an organization independent of DCSS. In addition to active intrusion detection, the IRT regularly runs vulnerability scans of all NIH host systems using the Security Auditor's Research Assistant (SARA) automated utility. The resultant reports are forwarded to all host system administrators for follow-up action. Administrators review the reports and take appropriate remedial actions in accordance with NIH policy. Also run IDS tool.

#### 3.6.5 Security Alerts and Advisories

\_X\_ In Place \_\_\_\_ Planned\_\_ In Place & Planned\_\_\_ Not Applicable

The Incident Response Team in OD CIO is responsible for the NIH-wide incident response capability. The IRT receives incident reports from its intrusion detection server and from individuals. The IRT informs the appropriate technical staff in the affected Institute or Center who take followup actions to investigate and respond to the incident. In addition to receiving alerts from the IRT, DCSS administrators regularly review host system logs, reports, and/or system alerts to ascertain apparent security breaches. NEES will be part of this process.

#### **3.6.6 Security Functionality and Verification**

\_\_\_ In Place \_\_\_ X\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

Planned to be in place.

#### 3.6.7 Software and Information Integrity

\_X\_ In Place \_\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

Critical system configurations, such as APF authorized libraries, supervisory calls, and exits are documented and periodically reviewed for appropriateness. Dedicated LSSB staff are assigned the responsibility to monitor critical parameters of various software products to ensure they are only changed when authorized. Not required for Moderate systems.

#### 3.6.8 Spam and Spyware Protection

\_X\_ In Place \_\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

Handled by CIT.

#### **3.6.9 Information Input Restrictions**

\_X\_ In Place \_\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

Non-public users requiring access to privileged information within the NEES database will be given an account according to the Account Creation/ Termination Policy. The non-public portion of NEES requires user authentication (login name and password) for NIH users and IBC reporters. Upon login, users will be given access to functionality and information appropriate to their assigned application role and organization. This is not a requirement for low impact systems.

# **3.6.10Information Input Accuracy, Completeness, and Validity** X In Place Planned In Place & Planned Not Applicable

Only registered NEES users with the proper associated user role will have the technical permissions needed to create, update or delete data. To preclude errors while entering data, a user will encounter numerous validation controls such as date checks and limited-value pick lists. NEES has reviewers in place.

#### **3.6.11Error Handling**

\_X\_ In Place \_\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

Log errors and handle errors go through applications.

#### **3.6.12Information Output Handling and Retention**

## \_X\_ In Place \_\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

NEES system owners handles and retains the output in accordance with all NIH policies and requirements.

## **3.7 MEDIA PROTECTION**

Organizations must: (i) protect information contained in organizational information systems in printed form or on digital media; (ii) limit access to information in printed form or on digital media removed from organizational information systems to authorized users; and (iii) sanitize or destroy digital media before disposal or release for reuse.

Input/output controls include measures to provide physical and environmental protection and accountability for tapes, diskettes, printouts, and other media. They include formal procedures for marking, handling, processing, storage, and disposal of input and output information and maintaining an audit trail. The level of sensitivity and criticality of data in printouts and storage media shall be identified. Printouts and storage media shall be stored, handled, or destroyed in accordance with their levels of sensitivity and criticality.

The Media Protection family consist of the following security controls:

- Media Protection Policies and Procedures
- Media Access
- Media Labeling
- Media Storage
- Media Transport
- Media Sanitization
- Media Destruction and Disposal

# 3.7.1 Media Protection Policies and Procedures

# \_X\_\_ In Place\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

See NIH Master Security Plan Section4.4, *Media Control* and NIH Sanitization Policy.

## 3.7.2 Media Access

# \_X\_ In Place\_\_\_ Planned\_\_ In Place & Planned\_\_ Not Applicable

All media at CIT containing sensitive information is appropriately labeled and secured away from general-purpose information. Only authorized personnel has access to this information.

## 3.7.3 Media Labeling

# \_X\_ In Place\_\_ Planned\_\_ In Place & Planned\_\_\_ Not Applicable

All storage media is properly labeled and stored within the CIT computer room.

#### 3.7.4 Media Storage

## \_\_\_ In Place\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

Handled by CIT.

## **3.7.5 Media Transport**

\_\_\_X\_\_In Place\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

## **3.7.6 Media Sanitization**

# \_X\_ In Place\_\_ Planned\_\_ In Place & Planned\_\_ Not Applicable

The Scientific Equipment and Instrumentation Branch (SEIB) will be provides sanitization services to the NIH community. Before any NIH-owned or managed hard disk or system containing a hard disk is transferred, surplused, or donated, it must be sanitized by reformatting the hard drive in a secure manner or by using an approved wipeout utility. Diskettes and other magnetic storage media that contain any government data or software must be sanitized when they are no longer needed. Portable media may be reused after overwriting or degaussing, or they may be destroyed. If the system will be donated to an outside organization, it should have a complete operating system installed on it after sanitization. See the NIH Sanitization Policy for further detail.

## 3.7.7 Media Destruction and Disposal \_\_X\_ In Place\_\_ Planned\_\_ In Place & Planned\_\_ Not Applicable

Hardcopy documentation that needs to be disposed of will be shredded while electronic media will be properly sanitized according to the NIH Sanitization Policy.

## 3.8 INCIDENT RESPONSE CAPABILITY

Organizations must: (i) establish an operational incident response capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.

Computer security incidents are becoming more common and their impact farreaching. When faced with an incident, NIH should be able to respond quickly in a manner that both protects its own information and helps to protect the information of others that might be affected by the incident. NIH will establish and maintain an incident response capability (the NIH IRT) to include preparation, identification, containment, eradication, recovery, and follow-up capabilities to ensure effective recovery from incidents. ICs shall document and report all security incidents to the NIH IRT, which will provide updates to the NIH CISO. The IRT and IC ISSOs will ensure that evidence of computer crimes is properly preserved.

The Incident Response Capability family consist of the following security controls:

- Incident Response Capability Policies and Procedures
- Incident Response Training
- Incident Response Testing
- Incident Handling
- Incident Monitoring
- Incident Reporting
- Incident Response Assistance

# 3.8.1 Incident Response Capability Policies and Procedures

\_X\_ In Place\_\_ Planned\_\_ In Place & Planned\_\_ Not Applicable

See NIH Master Security Plan Section 4.9.1, Security Incident and Violation Handling and NIH Vulnerability Scanning Policy and NIH Incident Handling Guidelines and NIH Incident Handling Procedures.

# 3.8.2 Incident Response Training

# \_X\_ In Place\_\_ Planned\_\_ In Place & Planned\_\_ Not Applicable

NIH shall train personnel in their incident response roles and responsibilities with respect to the information system and provide refresher training annually. Below lists the types of training to specific NIH personnel.

#### NIH Controls:

At NIH Incident Response training is provided in the following forms:

- To the Incident Response Team:
  - o Weekly meetings
  - Formal classroom training (e.g., SANS Institute, HHS University, and CIT)
  - o On-the-Job and Vendor training
- To the IC Incident Response staff (e.g. Information System Security Officers (ISSOs) and LAN Administrators):
  - Formal classroom training (e.g., SANS Institute, HHS University, and CIT)
  - Monthly ISSO meetings (which includes software tool, and NIH and vendor product demonstrations)
  - o IRT Alerts and Advisories (distributed and posted on the NIH IT Security web page)
  - o Daily federal government alerts (e.g., CIAC, CERT)
  - On-the-Job and Vendor training

## 3.8.3 Incident Response Testing

# \_X\_ In Place\_\_ Planned\_\_ In Place & Planned\_\_ Not Applicable

NIH shall test the incident response capability for the information system annually using at least simulation-level tests to determine the plan's effectiveness and document the results.

Testing includes:

- Simulated incident announcements to test response time.
- IRT sponsored periodic table talk exercises to test procedures and capabilities

# **3.8.4 Incident Handling**

\_X\_ In Place\_\_ Planned\_\_ In Place & Planned\_\_ Not Applicable

NIH has documented procedures, support tools, web-based tools, and a multi-faceted communication system between the ICs and divisions for incident handling.

The IRT proactively and reactively assures the security of NIH systems, data, and biomedical research information while maintaining connectivity and interoperability throughout NIH. The IRT identifies computer security incidents, characterizes the nature and severity of incidents, and provides immediate diagnostic and corrective actions when appropriate. When the IRT detects real or probable malicious activity, quick and effective action is applied to prevent unauthorized access to NIH systems and networks or minimize the impact of such activity. The IRT has a team of experts that is available to assist NIH system administrators with investigating incidents and repairing compromised systems 24 hours a day and seven days a week.

NIH shall incorporate the lessons learned from ongoing incident handling activities into the incident response procedures and implement the procedures accordingly. The NIH IRT (and IC response support staff) modifies support and response procedures whenever events/circumstances dictate that changes are needed.

In the event the NEES Application System Administrator suspects any unauthorized use or compromise to the NEES, he/she must contact the ISSO for review and reporting. The NEES System Administrator will assist the ISSO or any other authorized security personnel to assess whether any data has been added, modified or deleted. In addition, NEES will be checked for hidden files, deleted files, Trojan horses, etc., and then restored to its last known secure state.

## **3.8.5 Incident Monitoring**

# \_X\_ In Place\_\_ Planned\_ \_ In Place & Planned\_\_ Not Applicable

NIH performs this function via e-mail, databases, and ticketing systems (i.e. Remedy).

# 3.8.6 Incident Reporting

# \_X\_ In Place\_ Planned\_\_ In Place & Planned\_\_\_ Not Applicable

Supplemental Guidance: The types of incident information reported, the content and timeliness of the reports, and the list of designated reporting authorities or organizations are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance.

#### Control Enhancements:

(1) The organization employs automated mechanisms to assist in the reporting of security incidents.

The NIH IRT reports incidents to the appropriate authorities (i.e., HHS Secure One, FBI, NIH management, IC management, ISSOs, etc.) as applicable. Information about reporting requirements can be found in the <u>HHS Incident</u> <u>Response Planning Guide</u><sup>3</sup>.

The types of incident information reported, the content and timeliness of the reports, and the list of designated reporting authorities or organizations will be consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. NIH reports all incidents in a timely fashion according to HHS policy.

When a security incident occurs the ISSO is notified and is responsible for ensure the incident is responded to and resolved as appropriate which may include the notifying the NIH Police if required. A user may notify the ISSO directly but is encouraged to notify the CIT NIH Help desk online (<u>http://support.cit.nih.gov/</u>) or by phone (301-496-4357) to ensure that the incident is logged into Remedy for tracking (See Figure 2). Need something here.

<sup>&</sup>lt;sup>3</sup> <u>http://intranet.hhs.gov/infosec/docs/policies\_guides/IRP/Incident\_Response\_Planning\_Guide\_07192005.doc</u>



Figure 3: CIT NIH Help Desk Service Request Form

## 3.8.7 Incident Response Assistance

## \_X\_ In Place\_\_ Planned\_\_\_ In Place & Planned\_\_ Not Applicable

NIH provides an incident support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. Advice and assistance is provided to CIT IT Security Staff, IC ISSOs, LAN Administrators, and NIH management by e-mail, 24x7 hotline number, alerts & advisories, and web page with policies, procedures, guidance, checklists, forms, etc.

## 3.9 AWARENESS AND TRAINING

Organizations must: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, executive orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

The Computer Security Act requires federal agencies to provide for mandatory periodic training in computer security awareness and accepted computer security practices for all employees who are involved with the management, use, or operation of a federal computer system within or under the supervision of the federal agency.

All users of NIH information systems should be aware of Federal information security requirements and guidelines in order to protect agency information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. An initial information security awareness course followed by annual reviews, as well as supplemental IT security materials (e.g., articles, newsletters, posters) in the workplace educate users and remind them of their security responsibilities.

Role-based security training is required for personnel with significant information security responsibilities to ensure they possess the knowledge and skills needed to protect information and information systems. Security training should be tailored to each individual's role and responsibilities.

The Awareness and Training family consist of the following security controls:

- Awareness and Training Policies and Procedures
- Security Awareness
- Security Training
- Security Training Records

# 3.9.1 Awareness and Training Policies and Procedures \_\_X\_ In Place\_ Planned\_\_ In Place & Planned\_\_ Not Applicable

See NIH Master Security Plan section 4.1.7, *Security Education and Awareness* and NIH *Information Security Awareness and Training* Policy.

# 3.9.2 Security Awareness \_X\_ In Place\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

In addition to overall NIH security awareness training, NEES contains both a web-based training module and an online help module that will assist in the navigation and use of the system. All NEES users will be required to read and understand the NEES security policy on userid/password (included in the online user help). NEES users within NIH will receive training (in person) as needed when new functionality is added during software releases.

#### **3.9.3 Security Training**

## \_X\_ In Place\_\_ Planned\_\_ In Place & Planned\_\_ Not Applicable

NIH will receive training from the contractor on how to operate the web site, but no "technical" training on how to operate/manage SQL Server (for example) will be required. Users outside of NIH can take advantage of the web-based training module (presented on the NEES homepage), but this is not required to use the system.

According to NIH policy, all personnel who use NIH applications must attend security awareness training every year. All NIH personnel, contract personnel, and non-NIH users with authorized access to NIH-owned information system resources are required to complete NIH's on-line security awareness training course. NIH policy requires users annually to review an online security awareness training course. All other users must complete at a minimum an HHS approved annual security training course.

#### 3.9.4 Security Training Records

## \_X\_ In Place\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

The NIH training system maintains a log of users that have completed the training and the time of completion. In addition, all internal users are required to have completed the annual NIH Security Awareness Training, all users using Government resources are required to review and accept the NIH Rules of Behavior policy, and all users are required to familiarize themselves with NIH security procedures and policies. NEES users fall under this process.

## 4.TECHNICAL CONTROLS

Technical controls are those security measures executed by the system they protect. These controls can provide automated protection from unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. Technical controls are normally applied in layers to protect the confidentiality, integrity, and availability of the information handled by the system. According to NIST 800-53, the technical controls class consists of the following families:

- Identification and Authentication
- Access Controls
- Audit and Accountability
- Systems and Communication Protection

## 4.1 IDENTIFICATION AND AUTHENTICATION

Organizations must: (i) identify information system users, processes acting on behalf of users, or devices; and (ii) authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Identification and Authentication are technical controls that when used properly establish a basis for preventing unauthorized access to a system or application. Identification is the process of uniquely identifying oneself to a system or application. Identification can take the form of a User-ID; this User-ID is a unique identifier to the system or application. Authentication is the act of providing proof that you are who you claim to be – that can be something you know, something you have, something you are, or someplace you are.

FISMA requires that there be a process in place to uniquely identify each user, to verify users' identity, to receive authorization to issue a user identifier from appropriate officials, for issuing identifiers and authenticators to end users, and for disabling, removing, and archiving user identifiers and accounts.

The Identification and Authentication family consist of the following security controls:

- Identification and Authentication Policies and Procedures
- User Identification and Authentication
- Device Identification and Authentication
- Identifier Management
- Authenticator Management
- Authenticator Feedback
- Cryptographic Module Authentication

# 4.1.1 Identification and Authentication Policies and Procedures \_X\_ In Place\_\_ Planned\_\_ In Place & Planned\_\_ Not Applicable

See NIH Master Security Plan section 5.1, *Identification and Authentication*, NIH *User Password Requirements*, NIH *Password Policy*.

# 4.1.2 User Identification and Authentication \_X\_ In Place\_\_ Planned\_\_ In Place & Planned\_\_ Not Applicable

Each users login name is unique and will be assigned by the application during the registration process. Passwords will be stored in the application "account" table in encrypted format.

The application has been designed to ensure user passwords comply with NIH Policy. Policies stipulated in the NIH Password Policy as revised

January 21, 2005, and the NIH User Password Requirements as revised January 21, 2005 were used in designing the application. The NEES software enforces password compliance (that meets or exceeds the above referenced NIH policies) in the following ways:

- Length of password (7-20 characters)
- Password expiration (120 days)
- Mandatory inclusion of non-alphanumeric (i.e. "special") characters
- Mandatory inclusion of alphabetic characters
- Mandatory inclusion of at least one number
- Frequency of reuse, cannot repeat last 10 passwords
- Account expiration (inactivation) after 180 days.

# 4.1.3 Device Identification and Authentication

# \_\_\_ In Place\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

Handled by Single Sign On.

## 4.1.4 Identifier Management

\_\_X\_ In Place\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

Handled by Single Sign On.

# 4.1.5 Authenticator Management

\_X\_ In Place\_\_ Planned\_\_ In Place & Planned\_\_ Not Applicable

Handled by Single Sign On.

## 4.1.6 Authenticator Feedback

\_\_\_\_ In Place\_\_\_ Planned\_\_\_ In Place & Planned \_\_\_ Not Applicable

Not in place.

# 4.1.7 Cryptographic Module Authentication

\_X\_ In Place\_\_ Planned\_\_ In Place & Planned\_\_ Not Applicable

# 4.2 ACCESS CONTROLS

Organizations must limit: (i) information system access to authorized users, processes acting on behalf of authorized users or devices (including other information systems); and (ii) the types of transactions and functions that authorized users are permitted to exercise.

Access controls are system-based mechanisms used to specify who or what is to have access to a specific system resource and the type of access that is permitted. Practices are based on standards and procedures associated with user ID and authentication and access privileges to systems, databases, data fields and privileges to view, create, modify, and delete data.

The Logical Access Controls family consist of the following security controls:

- Access Control Policy and Procedures
- Account Management
- Access Enforcement
- Information Flow Enforcement
- Separation of Duties
- Least Privilege
- Unsuccessful login attempts
- System Use notification
- Previous Logon Notification
- Concurrent Session Control
- Session Lock
- Session Termination
- Supervision and Review Access Control
- Permitted Actions w/o Identification or Authentication
- Automated Marking
- Automated Labeling
- Remote Access
- Wireless Access Restrictions
- Access Control for Portable Mobile Systems
- Personally Owned Information Systems

## 4.2.1 Access Control Policy and Procedures

## \_X\_ In Place\_\_ Planned\_\_ In Place & Planned\_ Not Applicable

- Based on the NIH Master Security Plan section 5.2 *Access Control (Authorization),* each system is required to establish access control rules to be implemented to ensure only designated individuals, under specified conditions (e.g., time of day, port of entry, type of authentication, etc.) can:
  - Access the information system (e.g., log-on, establish connection).
  - Activate specific system commands.
  - Execute specific programs and procedures.
  - Create, view, or modify specific objects (e.g., programs, information, system parameters).

- Ensure that for information systems employing password-based authentication, passwords are:
  - one-way encrypted for storage
  - transmitted on the network in a secure manner (e.g., encrypted)
  - not displayed when entered
  - controlled by the associated user
  - overwritten in memory immediately following use
  - not displayed on user screen
- Ensure authentication is required for access to NIH systems from the Internet with the use of passwords as the minimum standard for authentication.
- Ensure that access to security software is restricted to security administrators.
- Implement controls to monitor access and identify apparent security violations.
- Ensure appropriate investigation procedures are implemented following security violations.

## 4.2.2 Account Management

# \_X\_ In Place\_\_ Planned\_\_ In Place & Planned\_ \_\_ Not Applicable

NEES uses role based management. Certain roles can add certain users. The highest level NIH administrator maintains all accounts. NIH administrator accounts are set by system administrators. Each institute designates filers and maintains any of the roles within their institute.

## 4.2.3 Access Enforcement

\_X\_ In Place\_\_ Planned\_\_ In Place & Planned\_ \_ Not Applicable

NEES employs Role-based user controls.

## 4.2.4 Information Flow Enforcement \_X\_ In Place\_\_ Planned\_\_ In Place & Planned\_\_ Not Applicable

Information Flow Enforcement is NEES Role-based.

# 4.2.5 Separation of Duties \_X\_ In Place\_\_ Planned\_\_ In Place & Planned\_\_ Not Applicable

For NEES, Separation of Duties is role-based.

## 4.2.6 Least Privilege

\_X\_ In Place\_\_ Planned\_\_ In Place & Planned\_\_ Not Applicable

#### 63 SENSITIVE

For NEES, Least Privilege is role-based.

# 4.2.7 Unsuccessful login attempts

# \_X\_ In Place\_\_ Planned\_\_ In Place & Planned\_\_ Not Applicable

Single Sign On.

# 4.2.8 System Use notification \_X\_ In Place\_\_ Planned\_\_ In Place & Planned\_\_ Not Applicable

A warning banner is in place at the single sign on window.

# 4.2.9 Previous Logon Notification \_\_\_\_ In Place\_\_\_ Planned\_\_\_ In Place & Planned \_X\_\_ Not Applicable

Not required for Moderate impact systems.

# 4.2.10Concurrent Session Control \_\_\_\_ In Place\_\_\_ Planned\_\_ In Place & Planned\_ X \_\_\_ Not Applicable

Not required for Moderate impact systems.

# 4.2.11 Session Lock

\_X\_ In Place\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

# 4.2.12Session Termination

# \_X\_ In Place\_\_ Planned\_\_ In Place & Planned\_\_ Not Applicable

NEES automatically terminates a session after 20 minutes of inactivity.

## 4.2.13Supervision and Review - Access Control \_\_\_\_\_ In Place\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

All access controls usage will be monitored and reviewed by the NIH Ethics Office and CIT personnel.

# 4.2.14Permitted Actions w/o Identification or Authentication \_X\_ In Place\_\_ Planned\_\_ In Place & Planned\_\_ Not Applicable

Users can submit feedback or questions (through the Contact Us page). In addition, one report will be available from the homepage for users not logged into the system that lists publicly available information. However, no sensitive

information (passwords only) can be accessible without proper identification and authentication.

### 4.2.15Automated Marking

# \_\_\_ In Place\_\_\_ Planned\_\_\_ In Place & Planned \_X\_\_ Not Applicable

Not required for Moderate impact systems.

### 4.2.16Automated Labeling In Place Planned In Place & Planned X Not Applicable

Not required for Moderate impact systems.

## 4.2.17Remote Access \_\_X\_ In Place\_\_ Planned\_\_ In Place & Planned\_\_ Not Applicable

NEES is a web based application, therefore, all users will be able to access the application remotely. Remote access occurs through a virtual private network. The monitoring of access to NEES will be monitored and logged by CIT and the NIH Ethics Office.

## 4.2.18Wireless Access Restrictions

\_\_\_ In Place\_\_\_ Planned\_\_\_ In Place & Planned \_X\_\_ Not Applicable

Not Applicable.

#### 4.2.19Access Control for Portable Mobile Systems In Place Planned In Place & Planned X Not Applicable

Not Applicable.

#### 4.2.20Personally Owned Information Systems X In Place Planned In Place & Planned Not Applicable

NEES internal users follow the NIH policy set forth in the Limited Authorized Personal Use of NIH Information Technology (IT) Resources policy.

# 4.3 AUDIT AND ACCOUNTABILITY

Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

The Audit and Accountability consist of the following controls:

- Audit and Accountability Policy and Procedures
- Auditable Events
- Content of Audit Records
- Audit Storage Capacity
- Audit Processing
- Audit Monitoring, Analysis, and Reporting
- Audit Reduction and Report Generation
- Time Stamps
- Protection of Audit Information
- Non-repudiation
- Audit Retention

# 4.3.1 Audit and Accountability Policy and Procedures \_X\_ In Place\_\_ Planned\_\_ In Place & Planned\_\_ Not Applicable

The NIH Master Security Plan requires NIH to:

- Maintain and protect audit logs.
- Ensure system and application audit logs record system activity by both system and application processes and user activities.
- Ensure audit logs record the following events:
- start-up and shutdowns of systems or audit functions
- successful and unsuccessful login and logout of users
- actions taken by system administrators, system security administrators, or other super users
- changes or attempts to change privileges and access controls for users and objects.
- Ensure audit logs record the following <u>information</u> for each event:
- date and time of the event
- type of event
- success or failure of the event
- name of the program or file introduced, accessed, modified, or deleted.
- Ensure systems are able to associate each auditable event with the individual identity of the user or system process that caused the event.
- For servers, ensure audit logs/records are backed up no less than weekly onto a different information system or media than the system being audited.
- Ensure audit logs are protected as sensitive information and retained for an appropriate time period.
- Ensure system administrators do not have "write" access to audit trails.
- A person other than the system administrator must conduct regular analyses of audit trails, although the system administrator may also be permitted to review audit trails.

## 4.3.2 Auditable Events

# \_X\_\_ In Place\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

If a single-sign on fails, a notification is sent. A notification is sent once a restored application is restarted. All actions are logged into a database.

## 4.3.3 Content of Audit Records

## \_X\_ In Place \_ Planned\_\_\_\_ In Place & Planned\_\_\_ Not Applicable

NEES captures the last update date, the users role, his full ID, and log exceptions/error ID. All URLs are hidden from the user. The user can only access what they are allowed to see based on their role.

## 4.3.4 Audit Storage Capacity

## \_X\_ In Place\_\_ Planned \_\_ In Place & Planned\_\_ Not Applicable

NEES does not have a limit on its audit storage capacity.

## 4.3.5 Audit Processing

## \_X\_ In Place\_\_\_ Planned \_\_\_ In Place & Planned\_\_\_\_ Not Applicable

After 6 years the reports are purged and anything having to do with the data is purged as well.

## 4.3.6 Audit Monitoring, Analysis, and Reporting

\_\_\_ In Place\_\_\_ Planned\_\_\_ In Place & Planned \_\_\_ Not Applicable

Not in place.

## 4.3.7 Audit Reduction and Report Generation

\_X\_ In Place\_\_ Planned\_\_ In Place & Planned\_\_ Not Applicable

The audits are categorized by action type.

## 4.3.8 Time Stamps \_X\_ In Place\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

Time stamps are provide for use in an audit record generation.

## 4.3.9 Protection of Audit Information \_X\_ In Place\_\_ Planned\_\_ In Place & Planned\_\_ Not Applicable

DBA is only person to delete or make changes and is the only one who has access.

## 4.3.10Non-repudiation

# \_\_\_ In Place\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

Not required for moderate impact systems.

## 4.3.11Audit Retention

## \_X\_ In Place\_\_ Planned\_\_ In Place & Planned\_\_ Not Applicable

The audit retention time is 6 years.

## 4.4 SYSTEMS AND COMMUNICATION PROTECTION

Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

Many of the Systems and Communications protection mechanisms are the responsibility of CIT as they pertain to protection of network boundaries, denial of service protection, network transmission integrity, and resource prioritization.

The Systems and Communication Protection family consists of the following controls:

- System and Communications Protection Policy and Procedures
- Application Partitioning
- Security Function Isolation
- Information Remnants

- Denial of Service Protection
- Resource Priority
- Boundary Protection
- Transmission Integrity
- Transmission Confidentiality
- Network Disconnect
- Trusted Path
- Cryptographic Key Establishment and Management
- Use of Validated Cryptography
- Public Access Protections
- Collaborative Computing
- Transmission of Security Parameters
- Public Key Infrastructure Certificates
- Mobile Code
- Voice Over Internet Protocol

# 4.4.1 System and Communications Protection Policy and Procedures \_X\_ In Place\_\_ Planned\_\_ In Place & Planned\_\_ Not Applicable

See NIH Master IT Security Plan section 5.4, Network Security and NIH Public and Private Network Policy.

## 4.4.2 Application Partitioning

## \_X\_ In Place\_\_ Planned\_\_ In Place & Planned\_\_ Not Applicable

NEES separated user functionality from management functionality.

## 4.4.3 Security Function Isolation

\_\_\_ In Place\_\_\_ Planned\_\_\_ In Place & Planned \_X\_ Not Applicable

Not required for moderate impact systems.

## 4.4.4 Information Remnants

\_\_\_ In Place\_\_\_ Planned\_\_\_ In Place & Planned\_\_ Not Applicable

It is prevented on all dedicated servers.

## 4.4.5 Denial of Service Protection

\_X\_ In Place\_\_\_ Planned\_\_\_ In Place & Planned\_\_ Not Applicable

Handled by CIT.

4.4.6 Resource Priority \_\_\_\_ In Place \_\_\_ Planned \_\_\_ In Place & Planned \_X\_ Not Applicable Not required for moderate impact systems.

# 4.4.7 Boundary Protection

\_X\_\_ In Place\_\_\_ Planned\_\_\_ In Place & Planned\_\_ Not Applicable

CIT manages boundary controls.

## 4.4.8 Transmission Integrity

\_X\_ In Place\_\_ Planned\_\_ In Place & Planned\_\_ Not Applicable

Protected by SSL.

## 4.4.9 Transmission Confidentiality

## \_\_X\_ In Place\_\_\_ Planned\_\_\_ In Place & Planned\_\_ Not Applicable

Protected by SSL.

## 4.4.10Network Disconnect \_X\_ In Place\_\_ Planned\_\_ In Place & Planned\_\_ Not Applicable

Terminated after 20 minutes.

# 4.4.11Trusted Path

# \_\_\_ In Place\_\_\_ Planned\_\_\_ In Place & Planned \_X\_ Not Applicable

Not required for moderate impact systems.

4.4.12Cryptographic Key Establishment and Management \_X\_ In Place\_\_ Planned\_\_ In Place & Planned\_\_ Not Applicable

Encrypted with password in web.config.file on production server and key is stored there.

## 4.4.13Use of Validated Cryptography \_X\_ In Place\_\_ Planned\_\_ In Place & Planned\_\_ Not Applicable

NEES performs all cryptographic operations using FIPS 140-2 modules. NEES also uses .net activitiation.

## 4.4.14 Public Access Protections

# \_\_X\_ In Place\_\_\_ Planned\_\_\_ In Place & Planned\_\_\_ Not Applicable

NEES protects the integrity of the information and applications.

## 4.4.15Collaborative Computing

\_\_\_\_ In Place\_\_\_ Planned\_\_\_ In Place & Planned\_X\_\_ Not Applicable

NEES does not use collaborative computing.

## 4.4.16Transmission of Security Parameters \_\_\_\_\_ In Place \_\_\_ Planned \_\_\_ In Place & Planned \_X\_\_ Not Applicable

Not required for moderate impact systems.

# 4.4.17Public Key Infrastructure Certificates \_X\_ In Place\_\_ Planned\_\_ In Place & Planned\_\_ Not Applicable

NEES adheres to NIH policy and procedures regarding to PKI certificates.

## 4.4.18Mobile Code

\_\_\_\_ In Place\_\_\_ Planned\_\_\_ In Place & Planned \_\_X\_\_ Not Applicable

Not Applicable.

## 4.4.19Voice Over Internet Protocol

\_\_\_\_ In Place\_\_\_ Planned\_\_\_ In Place & Planned \_\_X\_\_ Not Applicable

Not Applicable.

# 5. SYSTEM SECURITY PLAN STATEMENT OF APPROVAL

The undersigned have carefully reviewed the information in this security document. Based on this review, it has been determined that the documented security information is appropriate for this information system.

Signature:	NEES Project Manager
Date:	
Signature:	NEES Information System Owner
Date:	
Signature:	NEES ISSO
Date:	

# **APPENDICES**

# **APPENDIX A - ACRONYMS**

ATO	Authority to Operate
C&A	Certification and Accreditation
CA	Certification Authority
CIO	Chief Information Officer
CIT	Computer Information Technology
CV	Curricula Vitae
DAA	Designated Approving Authority
DCSS	Division of Computer System Services
FBI	Federal Bureau of Investigation
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
GSS	General Support System
HHS	Department of Health and Human Services
HR	Human Resources
IBC	Institutional Bio-safety Committee
IC	Institutes and Centers
IDS	Intrusion Detection System/Software
IRT	Incident Response Team
IIS	Internet Information Services
IP	Internet Protocol
ISSO	Information Systems Security Officer
IT	Information Technology
LOE	Level of Effort
MA	Major Application
NEES	NIH Ethics Enterprise System
NIAMS	National Institute of Arthritis and Musculoskeletal and Skin
Diseases	
NIH	National Institutes of Health
NIST	National Institute of Standards and Technology
OD	Office of the Director
OGC	Office of the General Council
OIT	Office of Information Technology
OMB	Office of Management and Budget
PDD	Presidential Decision Directive
PDF	Portable Document Format
PIA	Privacy Impact Assessment
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
POA&M	Plan Of Action and Milestones
SARA	Security Auditor's Research Assistant
SC	Security Category
SDLC	System Development Life Cycle

## A-1 SENSITIVE

SEIB	Scientific Equipment and Instrumentation Branch
SOMB	Systems Operations and Management Branch
SP	Special Publication
SSP	System Security Plan
ST&E	Security Testing and Evaluation
TCP	Transmission Control Protocol
UPS	Uninterruptible Power Supply
VOIP	Voice Over Internet Protocol

# **APPENDIX B - DOCUMENT HISTORY**

Version Number	Date	Description
1.0	August 25, 2006	Version 1.0 of the NEES SSP

# APPENDIX C - SELF ASSESSMENT

# APPENDIX D - SECURITY AND RISK ASSESSMENT REPORT

# APPENDIX E - PLAN OF ACTION AND MILESTONES

# APPENDIX F - ST& E PLAN AND PROCEDURES

## **APPENDIX G - RULES OF BEHAVIOR**

## Introduction

### What is the Purpose of The Rules of Behavior?

The intent of these NIH Rules of Behavior is to summarize laws and guidelines from various NIH and other Federal documents, most specifically OMB Circular A-130 and Section 208 of the E-Government Act of 2002. These guidelines should be used by all ICs as a basis for their own security plans.

#### What are Rules of Behavior?

Rules of Behavior are part of a comprehensive program to provide complete information security. These guidelines were established to hold users accountable for their actions and responsible for information security. Rules of Behavior establish standards of behavior in recognition of the fact that knowledgeable users are the foundation of a successful security program. Users need to understand that taking personal responsibility for the security of their computer and the data it contains is an essential part of their job.

#### Who is Covered by These Rules?

These rules extend to all NIH personnel and any other persons using IT equipment or accessing NIH systems under formally established agreements. This includes contractors and other federally funded users. All users should be fully aware of, and abide by, NIH security policies as well as related federal policy contained in the Privacy Act, Freedom of Information Act, and NIH Records Management Regulations.

#### What are the penalties for Non-compliance?

Users who do not comply with the prescribed Rules of Behavior, are subject to penalties that can be imposed under existing policy and regulations, including official, written reprimands, suspension of system privileges, temporary suspension from duty, removal from current position, termination of employment, and even criminal prosecution. NIH will enforce the use of penalties against any user who willfully violates any NIH or federal system security (and related) policy as appropriate.

These Rules of Behavior are founded on the principles described in the NIH published security policy and other regulatory documents such as the Code of Ethics for Government Employees, Office of Personnel Management regulations, Office of Management and Budget regulations and Standard of Conduct for Federal Employees. Therefore, these Rules of Behavior carry the same responsibility for compliance as the official documents cited above.

## **Accountability-General Requirements**

Users:

- Users should adhere to the DHHS Standards of Conduct and behave in an ethical, proficient, informed, and trustworthy manner.
- Do not attempt to override technical or management controls (i.e., carrying sensitive data home on a floppy disk without prior approval, etc.).

### F-1 SENSITIVE

- All users should complete the NIH Information Security Awareness Training prior to obtaining access to NIH systems and take the annual review course thereafter.
- Use virus protection software.
- Use only systems, software, and data for which you have authorization and use them only for official government business, or in accordance with the NIH Personal Use policy located at <a href="http://www3.od.nih.gov/oma/manualchapters/management/2806/">http://www3.od.nih.gov/oma/manualchapters/management/2806/</a>.
- Report security incidents, or any incidents of suspected fraud, waste or misuse of NIH systems to appropriate officials.
- Encrypt sensitive information when reasonable and worthwhile.
- Protect passwords from access by other individuals.
- Change passwords frequently. The frequency should be commensurate with the risk and criticality of the system, but should be no less often than every six months. The current NIH Password Policy can be found at <a href="http://irm.cit.nih.gov/policy/passwords.html">http://irm.cit.nih.gov/policy/passwords.html</a>.
- Protect confidential and/or sensitive information from disclosure.
- Protect government property from theft, destruction, or misuse.
- Do not remove computers from NIH premises unless authorized in accordance with NIH property management requirements.
- Individuals identified as having significant information privacy responsibilities must take the NIH Privacy Act (PA) training available at <a href="http://oma.od.nih.gov/ms/privacy/pa-training/index.asp">http://oma.od.nih.gov/ms/privacy/pa-training/index.asp</a>

#### Managers:

- Ensure that staff are given access to, and ample time to complete, the NIH Information Security Awareness Training and the annual review course.
- Ensure that staff who are required to take the PA course are given ample time to complete it.
- Ensure that staff has access to, and are aware of, all existing NIH and federal policies and procedures relevant to the use of NIH information technology resources.
- Ensure that staff follows system security policies, guidelines and procedures.

### **Remote Access Off-site Use of IT Resources**

- Use government resources for authorized purposes only, or in accordance with the NIH Personal Use policy located at <u>http://www3.od.nih.gov/oma/manualchapters/management/2806/</u>.
- Take precautions to secure government information and information resources.
- Do not alter the configuration, including installing software or peripherals, on government equipment unless authorized.

- Use only authorized licensed NIH software on government equipment unless authorized to do so according to the NIH Personal Use Policy.
- Adhere to all provisions or agreements related to off-site work.
- Use virus protection software on off-site systems and keep it up-to-date.
- Access sensitive information over the Internet only with prior approval from the IC ISSO or appropriate management official.
- Change passwords frequently.
- Protect passwords from access by other individuals, e.g., do not store passwords in login scripts, batch files, or elsewhere on the computer.

For more information, see the NIH Remote Access Policy at <u>http://www3.od.nih.gov/oma/</u> <u>manualchapters/management/2810/</u> and the NIH Remote Access Standards and procedures at <u>http://irm.cit.nih.gov/nihsecurity/NIH\_RAS\_Sec\_Stand\_Proc.doc</u>.

## Appropriate Use of the Internet and E-mail

- Refer to the Guidelines for Appropriate Use of the World Wide Web by NIH Employees at <a href="http://irm.cit.nih.gov/policy/guideli2.html">http://irm.cit.nih.gov/policy/guideli2.html</a>.
- Refer to the NIH Web Page Privacy Policy at <u>http://www1.od.nih.gov/oma/manualchapters/management/2805/.</u>
- Use the Internet for business purposes only when on official government time, or in accordance with the NIH Personal Use policy located at <u>http://www3.od.nih.gov/oma/</u> <u>manualchapters/management/2806/</u>.
- Be aware when navigating through the Internet; you may be moving from an area of controlled access into an area of unknown security controls.
- Report any security incidents to the appropriate officials.
- Do NOT send highly sensitive information via e-mail or fax, unless encrypted.
- Refer to <a href="http://oma.od.nih.gov/ms/records/rmanagement.html">http://oma.od.nih.gov/ms/records/rmanagement.html</a> for the latest guidance on records requirements for official e-mail records and facsimile documents, or contact your IC Records Management Officer.
- Protect copyrighted software and information in accordance with the conditions under which it is provided.
- All Contractor staff who have access to and use NIH e-mail must set up an Autosignature or electronic business card (v-card) on their computer and/or personal digital assistant (PDA) to visibly identify themselves as a contractor on all outgoing email messages, including those that are sent in reply and on messages that are forwarded to another user. For more information, see "New Requirements for NIH Contractor" Designations in Email located at http://irm.cit.nih.gov/policy/contractors.html

## Access Control

Users:

- Grant access to systems and data only to those who have an official need to know.
- Do not use your trusted position and access rights to exploit system controls or access data for any reason other than in the performance of official duties.
- Never share or compromise your password.
- Make alternative provisions for access to information during your absence to avoid the sharing of passwords.
- Include the following disclaimer on the fax cover sheet when sending faxes:

#### \*\*\*\*WARNING\*\*\*\*

The attached information may be confidential. It is intended only for the addressee(s) identified above. If you are not the addressee(s), or an employee or agent of the addressee(s), please note that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this fax in error, please destroy the document and notify the sender of the error. Thank you.

### Managers:

- Delete or reassign accounts as soon as users no longer require access.
- Plan for disaster recovery and contingency situations.
- Determine access levels based on the user's duties and need to know.

### Information Technology (IT) service providers:

IT service providers include (but are not limited to): system administrators, computer operators, system engineers, network administrators, LAN server administrators, those who have access to change control parameters for equipment and software, database administrators, those who control user passwords and access levels, and troubleshooters/system maintenance personnel. IT service providers must:

- Restrict system access to those persons needed to perform assigned duties.
- Ensure system users are aware of their responsibilities regarding access security.
- Plan for disaster recovery and contingency situations.
- Be certain proper software access controls are in place to ensure the security, integrity and privacy of data. Key players for ensuring PA controls are in place included: IC Privacy Act Coordinators, System Managers, ISSOs, Records Management Officers, Forms Management Officers, and Contract Officers.
- Post logon warning banners at all logon points to Government computers and systems where technically practical. The banner policy and an example can be found at <u>http://irm.cit.nih.gov/policy/warnbanners.html</u>.
- Set passwords for new accounts.

- Set expiration dates for accounts and passwords (passwords must be changed at least once every six months).
- Delete or reassign accounts as soon as users leave NIH.

#### Selecting Passwords:

The objective when choosing a password is to make it as difficult as possible for a cracker to make educated guesses about what you've chosen. This leaves him/her no alternative but a brute force search, trying every possible combination of letters, numbers, and punctuation. A search of this sort, even conducted on a machine that could try millions of passwords per second, would require many years to complete.

#### What Not to Use

- Don't use your login name, e.g., smithj, in any form (as-is, reversed, capitalized, doubled, etc.).
- Don't use your first or last name in any form.
- Don't use your spouse's or child's name.
- Don't use other information easily obtained about you. This includes license plate numbers, telephone numbers, social security numbers, the brand of your automobile, the name of the street you live on, etc.
- Don't use a password of all digits, or all the same letter. This significantly decreases the search time for a cracker.
- Don't use a word contained in English or foreign language dictionaries, spelling lists, or other lists of words.
- Don't use a password shorter than seven characters.

#### What to Use

- Do use a password with mixed-case alphabetics if the system password is casesensitive.
- Do use a password with non-alphabetic characters, e.g., digits or punctuation or combine with alphabetic characters, e.g., \$robot2!
- Do use a password that is easy to remember, so you don't have to write it down.
- Do use a password that you can type quickly, without having to look at the keyboard. This makes it harder for someone to steal your password by watching over your shoulder.

### **Information Management**

#### General Rules:

- Place only mission-oriented information on a public access system, including Internet Web pages, e-mail servers, and news groups.
- Ensure that appropriate management officials have approved information for public

### F-5 SENSITIVE

dissemination.

- Ensure that you do not disclose any sensitive or inappropriate information through the use of public access connections.
- When providing a Web page, a disclaimer should be displayed on the home page, or linked to on the Internet or Intranet. More information can be found at <u>http://irm.cit.nih.gov/policy/guideli2.html</u>.
- Persistent cookies or fill-in forms should never be used on a site to collect data from users unless pre-approved.
- Ensure that sensitive information sent to a fax or printer is handled in a secure manner, e.g., cover sheet to contain statement that information being faxed is confidential.
- Ensure electronic official records (including attachments) are printed and stored according to NARA's guidelines. Contact your IC Records Management Officer <u>http://oma.od.nih.gov/about/contact/browse.asp?fa\_id=2</u>.

### Specific Privacy Act Requirements:

- Know that information systems containing personally identifiable information (e.g., SSN, name, photo, and patient ID number) must be covered by a Privacy Act System of Records (SOR) Notice and will likely have added security controls you must follow. Read the Notice.
- Data collection forms and IC websites that collect personal information must include a PA Notification Statement that provides the authority and purpose for collecting the information, proposes uses, how and to whom the information may be disclosed, if the request is voluntary or mandatory, and any effect on the customer should they choose not to provide the information. Contact IC PA Coordinators for questions.
- Contracts covered by the PA must include a copy of the PA System Notice and the applicable Federal Acquisition Regulation (FAR) citations.
- Privacy Impact Assessments (PIA) must be completed on all electronic IT systems. Guidance is located at: <u>http://www.hhs.gov/pia/index.html</u>.
- Ensure that privacy policies are posted on agency websites used by the public.
- Privacy policies must be translated into a standardized machine-readable format.

#### Backing up Systems:

- Backups should be performed commensurate with the risk and criticality of the data.
- Ensure backups are successful and copies are kept off site.
- Ensure data can be easily restored when necessary.
- Ensure virus protection software is in use and is current.
- Follow up on reported security incidents in a timely manner.

### F-6 SENSITIVE

• Destroy backups when no longer needed.

Disposition of Sensitive Resources:

- Hard copies of highly sensitive information should be destroyed by pulping or shredding.
- Highly sensitive information stored on removable media should be entirely erased, or the disks destroyed. When disposing of, or transferring a computer system, erase all files from the hard drive by using a wipe out utility, or destroy the disk if necessary according to the NIH Records Management Guidelines. Please refer to the following URL for the current NIH Sanitization policy: http://irm.cit.nih.gov/security/sanitization.html.

Date published: 03/21/02

G-1 SENSITIVE

# APPENDIX I - CONTINGENCY PLAN

# APPENDIX J - CONFIGURATION MANAGEMENT PLAN

# **APPENDIX K - ADDITIONAL SECURITY DOCUMENTATION**

Will be added.

Security Awareness and Training for NIH staff and contractors is provided via an on-line training application that can be can accessed from the following web site:

## http://irtsectraining.nih.gov/

🗿 NIH Computer Security Awareness - Microsoft Internet Explorer			. 8 ×
File Edit View Favorites Tools Help			
$\Rightarrow$ Back $\bullet \Rightarrow \bullet \otimes$ $\bigcirc$ $\bigcirc$ $\bigcirc$ Search Bravorites $\bigcirc$ Media $\bigcirc$ $\bigcirc$ $\bigcirc$ $\bigcirc$ $\bigcirc$ $\bigcirc$ $\bigcirc$ $\bigcirc$			
Address 🙋 http://irtsectraining.nih.gov/	•	¢>Go	Links »
Google 🗸 security training NIH 🔄 👸 Search Web 🔹 🤯 🖙 1012 blocked 🔋 AutoFill 🔤 Options 🔗 👸 security 👸 training 👸 NIH			
🧟 AIM 🕤 🔄 🔍 Search 🖉 Highlight 🛛 🚴 AIM 👻 🔂 Games 🛛 🂝 Personals 🔹 🏠 Weather			
NIH Computer Security Awareness			<b>^</b>
• -Login for Users of NIH IT Resources (If just browsing, click on Public Access)			
First Name:			
Contact your ISSO if you do not get your previous tracking information at the top of the next screen.			
Proceed directly to Continue			
© - Public Access Connection Speed: ⊂ 56k dial-up © LAN			
Proceed directly to Continue			
Continue Cancel			
i Done	internet		
🏽 🛃 Start 🛛 🖉 Micro 🗐 Docu 🖉 NIH 🔄 Quick Launch 🚮 🖉 🖼 🔕 📴 🕲 🙆 🐼 🐉 🎱 🗮 🎊 😫 🍭 🥔 🄌 👋 👋 👋 🛞	<mark>8</mark> 54	2:0	)4 PM