Form Report, printed by: Milliard, Suzanne, **Aug 24, 2010**

PIA SUMMARY

1

The following required questions with an asterisk (*) represent the information necessary to complete the PIA Summary for transmission to the Office of Management and Budget (OMB) and public posting in accordance with OMB Memorandum (M) 03-22.

Note: If a question or its response is not applicable, please answer "N/A" to that question where possible. If the system hosts a website, the Website Hosting Practices section is required to be completed regardless of the presence of personally identifiable information (PII). If no PII is contained in the system, please answer questions in the PIA Summary Tab and then promote the PIA to the Senior Official for Privacy who will authorize the PIA. If this system contains PII, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

2 Summary of PIA Required Questions

**Is this a new PIA?*

No

If this is an existing PIA, please provide a reason for revision:

PIA Validation

**1. Date of this Submission:*

Jul 30, 2010

**2. OPDIV Name:*

NIH

**4. Privacy Act System of Records Notice (SORN) Number (If response to Q.21 is Yes, a SORN number is required for Q.4):*

09-25-0200

**5. OMB Information Collection Approval Number:*

0925-0594

**6. Other Identifying Number(s):*

Z01 CP010196

**7. System Name (Align with system item name):*

NIH NCI AARP Phase I Pilot Study (APS)

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

Point of Contact Information	
POC Name	Yikyung Park

**10. Provide an overview of the system:*

The APS is a web-based system that manages the data collection activities related to the completion of four web-based instruments that capture dietary, physical activity and health information. The APS allows for a respondent to consent and complete a self-enrollment process. Enrollment includes the collection of contact information. Upon successful enrollment, respondents are assigned instruments to complete and a schedule by which to complete. Access to the instruments is granted to respondent based on assigned schedule. Email, text messaging, and automated phone calls are generated to remind respondents of upcoming and overdue events.

**13. Indicate if the system is new or an existing one being modified:*

New

**17. Does/Will the system collect, maintain (store), disseminate and/or pass through PII within any database(s), record(s), file(s) or website(s) hosted by this system?*

Note: This question seeks to identify any, and all, personal information associated with the system. This includes any PII, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. If the information contained in the system ONLY represents federal contact data (i.e., federal contact name, federal address, federal phone number, and federal email address), it does not qualify as PII, according to the E-Government Act of 2002, and the response to Q.17 should be No (only the PIA Summary

is required). If the system contains a mixture of federal contact information and other types of PII, the response to Q.17 should be Yes (full PIA is required).

Yes

17a. Is this a GSS PIA included for C&A purposes only, with no ownership of underlying application data? If the response to Q.17a is Yes, the response to Q.17 should be No and only the PIA Summary must be completed.

*19. Are records on the system retrieved by 1 or more PII data elements?

Yes

*21. Is the system subject to the Privacy Act? (If the response to Q.19 is Yes, the response to Q.21 must be Yes and a SORN number is required for Q.4)

Yes

*23. If the system shares or discloses PII, please specify with whom and for what purpose(s):

IIF will not be shared nor disclosed. This collection is covered under System of Records Notice 09-25-0200.

*30. Please describe in detail: (1) The information the agency will collect, maintain, or disseminate (clearly state if the information contained in the system ONLY represents federal contact data); (2) Why and for what purpose the agency will use the information; (3) Explicitly indicate whether the information contains PII; and (4) Whether submission of personal information is voluntary or mandatory:

Respondents will be asked for their name, email address and phone numbers as part of the study conduct to send reminders of upcoming events via outgoing automated outgoing phone calls, cell phone text messaging and email. Respondents can opt-out of cell phone text message and automated phone call reminders.
Phone numbers are also collected for use of providing support to study respondents.
Date of birth is collected to verify enrollment criteria (>50 yrs of age) as well to characterize respondent when determining aggregate response rates.
Race, ethnicity, and state are also collected to characterize respondent.
Social security number is collected for a subset of the respondents in order to determine the response rates and the likelihood in any main study of being able to link to cancer and other health registries for endpoint analyses.
The following fields are required:
Gender, OMB race category(ies), ethnicity, first and last names, mailing address, email, and social security number for a subset of respondents.
Participation is voluntary.

*31. Please describe in detail any processes in place to: (1) Notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of the original collection); (2) Notify and obtain consent from individuals regarding what PII is being collected from them; and (3) How the information will be used or shared. (Note: Please describe in what format individuals will be given notice of consent [e.g., written notice, electronic notice, etc.]):

The scope of the feasibility study is limited and there are no plans to make any major changes to the system. In the event of any changes that impact IIF, respondents will be notified via email of a change and be directed to log into their APS account for details or contact the APS helpdesk.
The consent text included in the system specifies what IIF is being collected and how it will be used or shared. Additionally, the systems includes frequently asked questions (FAQS) that further explain how IIQ information is stored and will be used.

*32. Does the system host a website? (Note: If the system hosts a website, the Website Hosting Practices section is required to be completed regardless of the presence of PII)

Yes

*37. Does the website have any information or pages directed at children under the age of thirteen?

No

*50. Are there policies or guidelines in place with regard to the retention and destruction of PII? (Refer to the C&A package and/or the Records Retention and Destruction section in SORN)

Yes

*54. Briefly describe in detail how the PII will be secured on the system using administrative, technical, and physical controls:

The following classes of controls are in place to protect the APS and respondent IIF: access such as user account management, access enforcement, password strength, least privilege concept, session termination; security awareness and training; audit and accountability; configuration management; contingency planning; identification and authentication for users, devices; incident response including training, testing, monitoring; timely and controlled maintenance; media protection; physical and environment controls such as id badges, physical access authorization using access cards, key locks and cipher locks for building and room entry, monitoring, visitor control, emergency power, and shutoff, disaster protection and recovery; system security plan; personnel security; rules of behavior; risk assessment planning, monitoring, update; technical and communication protection including denial of service protection; boundary protection, programmable firewalls, transmission integrity; security certificates, encryption, regular virus detection and monitoring; policies and procedures are in place for each family control class

PIA REQUIRE INFORMATION

1 HHS Privacy Impact Assessment (PIA)

The PIA determines if Personally Identifiable Information (PII) is contained within a system, what kind of PII, what is done with that information, and how that information is protected. Systems with PII are subject to an extensive list of requirements based on privacy laws, regulations, and guidance. The HHS Privacy Act Officer may be contacted for issues related to Freedom of Information Act (FOIA) and the Privacy Act. Respective Operating Division (OPDIV) Privacy Contacts may be contacted for issues related to the Privacy Act. The Office of the Chief Information Officer (OCIO) can be used as a resource for questions related to the administrative, technical, and physical controls of the system. Please note that answers to questions with an asterisk (*) will be submitted to the Office of Management and Budget (OMB) and made publicly available in accordance with OMB Memorandum (M) 03-22.

Note: If a question or its response is not applicable, please answer "N/A" to that question where possible.

2 General Information

**Is this a new PIA?*

No

If this is an existing PIA, please provide a reason for revision:

PIA Validation

**1. Date of this Submission:*

Jul 30, 2010

**2. OPDIV Name:*

NIH

3. Unique Project Identifier (UPI) Number for current fiscal year (Data is auto-populated from the System Inventory form, UPI table):

**4. Privacy Act System of Records Notice (SORN) Number (If response to Q.21 is Yes, a SORN number is required for Q.4):*

09-25-0200

**5. OMB Information Collection Approval Number:*

0925-0594

5a. OMB Collection Approval Number Expiration Date:

**6. Other Identifying Number(s):*

Z01 CP010196

**7. System Name: (Align with system item name)*

NIH NCI AARP Phase I Pilot Study (APS)

8. System Location: (OPDIV or contractor office building, room, city, and state)

System Location:	
OPDIV or contractor office building	Westat 1650 Research Blvd
Room	Server room
City	Rockville
State	MD

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

Point of Contact Information	
POC Name	Yikyung Park

The following information will not be made publicly available:

POC Title	Staff scientist
POC Organization	NIH/NCI
POC Phone	301-594-6394
POC Email	parkyik@mail.nih.gov

**10. Provide an overview of the system: (Note: The System Inventory form can provide additional information for child dependencies if the system is a GSS)*

The APS is a web-based system that manages the data collection activities related to the completion of four web-based instruments that capture dietary, physical activity and health information. The APS allows for a respondent to consent and complete a self-enrollment process. Enrollment includes the collection of contact information. Upon successful enrollment, respondents are assigned instruments to complete and a schedule by which to complete. Access to the instruments is granted to respondent based on assigned schedule. Email, text messaging, and automated phone calls are generated to remind respondents of upcoming and overdue events.

SYSTEM CHARACTERIZATION AND DATA CATEGORIZATION

1	System Characterization and Data Configuration

11. Does HHS own the system?

Yes

11a. If no, identify the system owner:

12. Does HHS operate the system? (If the system is operated at a contractor site, the answer should be No)

No

12a. If no, identify the system operator:

Westat, as NCI/DCEG/NEB's contractor, will operate APS

**13. Indicate if the system is new or an existing one being modified:*

New

14. Identify the life-cycle phase of this system:

Development/Acquisition

15. Have any of the following major changes occurred to the system since the PIA was last submitted?

No

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

16. Is the system a General Support System (GSS), Major Application (MA), Minor Application (child) or Minor Application (stand-alone)?

Minor Application (child)

**17. Does/Will the system collect, maintain (store), disseminate and/or pass through PII within any database(s), record(s), file(s) or website(s) hosted by this system?*

Yes

Note: This question seeks to identify any, and all, personal information associated with the system. This includes any PII, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. If the information contained in the system ONLY represents business contact data (i.e., business contact name, business address, business phone number, and business email address), it does not qualify as PII, according to the E-Government Act of 2002, and the response to Q.17 should be No (only the PIA Summary is required). If the system contains a mixture of business contact information and other types of PII, the response to Q.17 should be Yes (full PIA is required).

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

Categories:	Yes/No
Name (for purposes other than contacting federal	Yes

employees)	
Date of Birth	Yes
Social Security Number (SSN)	Yes
Photographic Identifiers	No
Driver's License	No
Biometric Identifiers	No
Mother's Maiden Name	No
Vehicle Identifiers	No
Personal Mailing Address	Yes
Personal Phone Numbers	Yes
Medical Records Numbers	No
Medical Notes	No
Financial Account Information	No
Certificates	No
Legal Documents	No
Device Identifiers	No
Web Uniform Resource Locator(s) (URL)	No
Personal Email Address	Yes
Education Records	No
Military Status	No
Employment Status	No
Foreign Activities	No
Other	

17a. Is this a GSS PIA included for C&A purposes only, with no ownership of underlying application data? If the response to Q.17a is Yes, the response to Q.17 should be No and only the PIA Summary must be completed.

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

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

**19. Are records on the system retrieved by 1 or more PII data elements?*

Yes

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

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

20. Are 10 or more records containing PII maintained, stored or transmitted/passed through this system?

Yes

**21. Is the system subject to the Privacy Act? (If the response to Q.19 is Yes, the response to Q.21 must be Yes and a SORN number is required for Q.4)*

Yes

21a. If yes but a SORN has not been created, please provide an explanation.

INFORMATION SHARING PRACTICES

1 Information Sharing Practices

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

No

Please indicate "Yes" or "No" for each category below:	Yes/No
Name (for purposes other than contacting federal employees)	
Date of Birth	
SSN	
Photographic Identifiers	
Driver's License	
Biometric Identifiers	
Mother's Maiden Name	
Vehicle Identifiers	
Personal Mailing Address	
Personal Phone Numbers	
Medical Records Numbers	
Medical Notes	
Financial Account Information	
Certificates	
Legal Documents	
Device Identifiers	
Web URLs	
Personal Email Address	
Education Records	
Military Status	
Employment Status	
Foreign Activities	
Other	

**23. If the system shares or discloses PII please specify with whom and for what purpose(s):*

IIF will not be shared nor disclosed. This collection is covered under System of Records Notice 09-25-0200.

24. If the PII in the system is matched against PII in one or more other computer systems, are computer data matching agreement(s) in place?

Not Applicable

25. Is there a process in place to notify organizations or systems that are dependent upon the PII contained in this system when major changes occur (i.e., revisions to PII, or when the system is replaced)?

Not Applicable

26. Are individuals notified how their PII is going to be used?

Yes

26a. If yes, please describe the process for allowing individuals to have a choice. If no, please provide an explanation.

After reading the consent and the specifics on how their IIF will be used, individuals can choose to participate in the research study or not.

27. Is there a complaint process in place for individuals who believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate?

Yes

27a. If yes, please describe briefly the notification process. If no, please provide an explanation.

Study respondents can submit complaints, concerns, and questions to the study helpdesk via email or phone

28. Are there processes in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy?

Yes

28a. If yes, please describe briefly the review process. If no, please provide an explanation.

Timely monitoring and quality control reports are run.

29. Are there rules of conduct in place for access to PII on the system?

Yes

Please indicate "Yes," "No," or "N/A" for each category. If yes, briefly state the purpose for each user to have access:

Users with access to PII	Yes/No/N/A	Purpose
User	Yes	To modify their own IIF
Administrators	Yes	To monitor and support the system; access and viewing of data is incidental to rendering services in order to diagnose and repair problems or to retrieve or repair data files.
Developers	Yes	Access needed to troubleshoot or maintain system; access and viewing of data is incidental to rendering services in order to diagnose and repair problems or to retrieve or repair data files.
Contractors	Yes	To administer, operate, and maintain the system; provide assistance and perform helpdesk functions and user support
Other		

**30. Please describe in detail: (1) The information the agency will collect, maintain, or disseminate (clearly state if the information contained in the system ONLY represents federal contact data); (2) Why and for what purpose the agency will use the information; (3) Explicitly indicate whether the information contains PII; and (4) Whether submission of personal information is voluntary or mandatory:*

Respondents will be asked for their name, email address and phone numbers as part of the study conduct to send reminders of upcoming events via outgoing automated outgoing phone calls, cell phone text messaging and email. Respondents can opt-out of cell phone text message and automated phone call reminders.
Phone numbers are also collected for use of providing support to study respondents.
Date of birth is collected to verify enrollment criteria (>50 yrs of age) as well to characterize respondent when determining aggregate response rates.
Race, ethnicity, and state are also collected to characterize respondent.
Social security number is collected for a subset of the respondents in order to determine the response rates and the likelihood in any main study of being able to link to cancer and other health registries for endpoint analyses.
The following fields are required:
Gender, OMB race category(ies), ethnicity, first and last names, mailing address, email, and social security number for a subset of respondents.
Participation is voluntary.

**31. Please describe in detail any processes in place to: (1) Notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of the original collection); (2) Notify and obtain consent from individuals regarding what PII is being collected from them; and (3) How the information will be used or shared. (Note: Please describe in what format individuals will be given notice of consent [e.g., written notice, electronic notice, etc.])*

The scope of the feasibility study is limited and there are no plans to make any major changes to the system. In the event of any changes that impact IIF, respondents will be notified via email of a change and be directed to log into their APS account for details or contact the APS helpdesk.
The consent text included in the system specifies what IIF is being collected and how it will be used or shared. Additionally, the systems

includes frequently asked questions (FAQS) that further explain how IIQ information is stored and will be used.

WEBSITE HOSTING PRACTICES

1 Website Hosting Practices

**32. Does the system host a website? (Note: If the system hosts a website, the Website Hosting Practices section is required to be completed regardless of the presence of PII)*

Yes

Please indicate "Yes" or "No" for each type of site below. If the system hosts both Internet and Intranet sites, indicate "Yes" for "Both" only.	Yes/ No	If the system hosts an Internet site, please enter the site URL. Do not enter any URL(s) for Intranet sites.
Internet	No	
Intranet	Yes	
Both	No	

33. Does the system host a website that is accessible by the public and does not meet the exceptions listed in OMB M-03-22?

Note: OMB M-03-22 Attachment A, Section III, Subsection C requires agencies to post a privacy policy for websites that are accessible to the public, but provides three exceptions: (1) Websites containing information other than "government information" as defined in OMB Circular A-130; (2) Agency intranet websites that are accessible only by authorized government users (employees, contractors, consultants, fellows, grantees); and (3) National security systems defined at 40 U.S.C. 11103 as exempt from the definition of information technology (see section 202(i) of the E-Government Act.).

Yes

34. If the website does not meet one or more of the exceptions described in Q. 33 (i.e., response to Q. 33 is "Yes"), a website privacy policy statement (consistent with OMB M-03-22 and Title II and III of the E-Government Act) is required. Has a website privacy policy been posted?

Yes

35. If a website privacy policy is required (i.e., response to Q. 34 is ''Yes''), is the privacy policy in machine-readable format, such as Platform for Privacy Preferences (P3P)?

No

35a. If no, please indicate when the website will be P3P compliant:

not planned due to the short period of study

36. Does the website employ tracking technologies?

Yes

Please indicate "Yes", "No", or "N/A" for each type of cookie below:	Yes/No/N/A
Web Bugs	No
Web Beacons	No
Session Cookies	Yes
Persistent Cookies	No
Other	no

**37. Does the website have any information or pages directed at children under the age of thirteen?*

No

37a. If yes, is there a unique privacy policy for the site, and does the unique privacy policy address the process for obtaining parental consent if any information is collected?

38. Does the website collect PII from individuals?

Yes

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

39. Are rules of conduct in place for access to PII on the website?

Yes

40. Does the website contain links to sites external to HHS that owns and/or operates the system?

No

40a. If yes, note whether the system provides a disclaimer notice for users that follow external links to websites not owned or operated by HHS.

ADMINISTRATIVE CONTROLS

1	Administrative Controls

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

41. Has the system been certified and accredited (C&A)?

No

41a. If yes, please indicate when the C&A was completed (Note: The C&A date is populated in the System Inventory form via the responsible Security personnel):

41b. If a system requires a C&A and no C&A was completed, is a C&A in progress?

Not Applicable

42. Is there a system security plan for this system?

Yes

43. Is there a contingency (or backup) plan for the system?

Yes

44. Are files backed up regularly?

Yes

45. Are backup files stored offsite?

Yes

46. Are there user manuals for the system?

Yes

47. Have personnel (system owners, managers, operators, contractors and/or program managers) using the system been trained and made aware of their responsibilities for protecting the information being collected and maintained?

Yes

48. If contractors operate or use the system, do the contracts include clauses ensuring adherence to privacy provisions and practices?

Yes

49. Are methods in place to ensure least privilege (i.e., ''need to know'' and accountability)?

Yes

49a. If yes, please specify method(s):

Security administrators restrict user, processes, application, and object privileges by setting the permission levels and privileges of through group and individual rights assignment based on roles, responsibilities, and function

**50. Are there policies or guidelines in place with regard to the retention and destruction of PII? (Refer to the C&A package and/or the Records Retention and Destruction section in SORN):*

Yes

50a. If yes, please provide some detail about these policies/practices:

The investigators will determine the retention period based on analysis requirements and timeline. The contractor operating and supporting the APS will use a proprietary tool to manage the retention period for the data and the destruction of archived files in accordance with best professional practices and project requirements. Listings of all archive tapes with expiring data retention review dates are reviewed semi-annually. Tapes designated for destruction by researchers are sent to a security vendor where they are physically destroyed, and the vendor sends a letter certifying the physical destruction of the specified tape. Shredding is the method by which the proper destruction of sensitive hard-copy documents is ensured.

TECHNICAL CONTROLS

1 Technical Controls

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

Yes

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

52. Is there a process in place to monitor and respond to privacy and/or security incidents?

Yes

52a. If yes, please briefly describe the process:

As outlined in the GSS Security Plan, there is an Incident Response Plan that provides detailed procedures for handling a security incident to minimize any adverse impact on the study and its participants.
Briefly the process contains these phases:
Preparation. Ensure that all system staff are aware of the plan, and ensure that the plan is regularly tested
Detection and Notification. Detect and assess the incident and activate the notification tree
Containment and Eradication. Isolate any affected system components, gather evidence, and restore system security safeguards
Recovery. Restore normal operations

All incidents will be included in a quarterly security report. Any weaknesses discovered as the result of an incident will be added to the system POA&M. Significant security incidents will be reported within four hours. Incidents involving personally identifying information will be reported immediately, so as to meet OMB reporting requirements.

PHYSICAL ACCESS

1 Physical Access

53. Are physical access controls in place?

Yes

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

**54. Briefly describe in detail how the PII will be secured on the system using administrative, technical, and physical controls:*

The following classes of controls are in place to protect the APS and respondent IIF: access such as user account management, access enforcement, password strength, least privilege concept, session termination; security awareness and training; audit and accountability; configuration management; contingency planning; identification and authentication for users, devices; incident response including training, testing, monitoring; timely and controlled maintenance; media protection; physical and environment controls such as id badges, physical access authorization using access cards, key locks and cipher locks for building and room entry, monitoring, visitor control, emergency power, and shutoff, disaster protection and recovery; system security plan; personnel security; rules of behavior; risk assessment planning, monitoring, update; technical and communication protection including denial of service protection; boundary protection, programmable firewalls, transmission integrity; security certificates, encryption, regular virus detection and monitoring; policies and procedures are in place for each family control class

APPROVAL/DEMOTION

1	System Information
System Name:	NIH NCI AARP Phase I Pilot Study (APS)

2	PIA Reviewer Approval/Promotion or Demotion
Promotion/Demotion:	Promote
Comments:	
Approval/Demotion Point of Contact:	Suzy Milliard
Date:	Jul 30, 2010

3	Senior Official for Privacy Approval/Promotion or Demotion
Promotion/Demotion:	Promote
Comments:	

4	OPDIV Senior Official for Privacy or Designee Approval

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

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

Name: _____ **Date:** _____

Name:	Karen Plá
Date:	Aug 11, 2009

5	Department Approval to Publish to the Web
Approved for web publishing	Yes
Date Published:	Sep 1, 2009
Publicly posted PIA URL or no PIA URL explanation:	

PIA % COMPLETE

1	PIA Completion
PIA Percentage Complete:	100.00
PIA Missing Fields:	