US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

07/17/2025

OPDIV:

NIH

Name:

NIA GSS: Aging Data Administration Management System

PIA Unique Identifier:

P-6082592-778631

The subject of this PIA is which of the following?

Minor Application (stand-alone)

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

No

Does the system include a Website or online application available to and for the use of the general public?

No

Identify the operator.

Agency

Is this a new or existing system?

Existing

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

PIA Validation

Describe in further detail any changes to the system that have occurred since the last PIA.

This validation is intended to refresh content. There have been no substantial changes since the last assessment.

Describe the purpose of the system.

The National Institute on Aging (NIA) Aging Data Administration Management System (ADAMS) is grant system that facilitates the ability to enter program classification codes (PCC) for competing applications prior to council meetings, scientifically code grants based on their study, search for grants, and run basic ad hoc queries from electronic Research Administration (eRA), the centralized NIH data system.

ADAMS modules include:
Coding On Demand System (CODSys),
NIA Research Portfolio Reporting and Tracking System (RPRTS), and

PCC Reassignment (PCC-R).

Describe the type of information the system will collect, maintain (store), or share.

ADAMS downloads current and historical information on grant applications and contracts awarded by the NIH, including contract performance evaluations from the source system Electronic Research Administration (eRA). This information is used to support centralized grant programs and contract management.

Information collected and/or stored include Grant title and/or contract number, private investigator's name, council date, study section, and priority score. No other personally identifiable information (PII) is collected, maintained, or stored.

Those requiring access to ADAMS log in using the NIH Identity, Credential, and Access Management Services (IAM), which maintains its own unique privacy impact assessment (PIA) on record, including all legal authorities documented. The purpose of the IAM is to authenticate and authorize all users and computers in a Windows domain type network, assigning and enforcing information security policies for all computers and installing or updating software. The IAM collects unique user credentials and stores them in an encrypted format. The IAM is an essential service which facilitates and governs network access to various resources.

eRA maintains its own unique PIA on record, with all legal authorities documented.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

The NIA ADAMS is grant system that facilitates the ability to enter program classification codes for competing applications prior council meetings, scientifically code grants based on their study, search for grants, and run basic ad hoc queries from eRA, the centralized NIH data system.

ADAMS downloads current and historical information on grant applications and contracts awarded by the NIH, including contract performance evaluations from eRA. This information is used to support centralized grant programs and contract management. Information collected and stored may include Grant title and/or contract number, private investigator's name, council date, study section, and score. No other PII is collected, maintained or stored.

ADAMS includes the following:
PCC Reassignment (PCC-R) module provides the ability to submit applications for PCC Reassignment for both competing and non-competing applications and Program Officers.
Coding on Demand (CODSys) includes program class codes .
NIA Research Portfolio Reporting and Tracking (NIA RPRTS) assigns scientific codes to grant records.

Those requiring access to ADAMS log in using the NIH IAM, which maintains its own unique PIA on record, including all legal authorities documented. The eRA maintains its own unique PIA on record, with all legal authorities documented.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Name
Council date, Contract number, Grant title
Study section, priority score

Contract performance evaluations

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees
Public Citizens
Business Partner/Contacts (Federal/state/local agencies)
No

How many individuals' PII is in the system?

50,000-99,999

For what primary purpose is the PII used?

Information is used to specify a particular grant.

Describe the secondary uses for which the PII will be used.

N/A

Identify legal authorities governing information use and disclosure specific to the system and program.

42 U.S.C.§ 241
42 U.S. Code § 282
42 U.S. Code § 284
42 USC § 285e

Are records on the system retrieved by one or more PII data elements?

Yes

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.

09-25-0225, NIH Electronic Research Administration (eRA)

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
Online
Government Sources
Within the DOC
Non-Government Sources
Public
Identify the OMB information collection approval number and expiration date
N/A. A collection approval number is not required as ADAMS is not surveying or soliciting information.

Is the PII shared with other organizations?

No

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

Information is gathered from eRA, the source system and maintains its own PIA. It is the responsibility of eRA to notify individuals.

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.

Information is gathered from eRA, the source system. It is the responsibility of eRA to allow for individuals to opt out.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

There is no process to notify and obtain consent from the individuals when major system changes occur because the information is gathered from eRA, which maintains its own PIA.

Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.

Individuals may contact eRA system owners or contact the NIH Senior Official for Privacy.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

ADAMS uses an application programming interface (API) web service to synchronize the data daily with the source system, eRA. Audit logs are stored in the system as part of the server access.

Identify who will have access to the PII in the system and the reason why they require access.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

Access is assigned to personnel based upon current job responsibilities. The system uses specific login information to assign permissions/user roles which may be considered PII. The NIH IAM combines the identity and authentication tools and capabilities used throughout the NIH enterprise.

Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.

Access to PII is assigned to personnel based upon current job responsibilities. A NIH IAM account is required to gain access to the stored PII data.

Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.

According to NIH policy, all personnel who manage or operate NIH applications must successfully complete annual security awareness training.

Describe training system users receive (above and beyond general security and privacy awareness training).

Administrators and Privileged Users require additional training specific to their roles and responsibilities.

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

Records are retained and disposed of under the authority of the NIH Records Retention Schedule.

Item 02-002, Official case files of funded grants, unfunded grants, and award applications, appeals and litigation records.
Cut off annually following completion of final grant-related activity that represents closing of the case file (e.g., end of project period, completed final peer review, litigation or appeal proceeding concluded). Destroy 10 years after cut-off (DAA-0443-2013-0004-0002).

Item 02-004, Extramural program and grants management oversight records. Cut off annually. Destroy 3 years after cut-off (DAA-0443-2013-0004-0004).

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

Physical controls include guards within NIH Data Centers, Identification (ID) badges, key cards and closed-circuit television (TV).

Technical controls include user ID, passwords, firewalls, Virtual Private Network (VPN).

Administrative controls include system security and contingency plan, contract clauses ensure adherence to privacy provisions and practices, least privilege through role-based access, and policies for retention and destruction of PII.