US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/16/2025

OPDIV:

NIH

Name:

NIH Enterprise Ethics System

PIA Unique Identifier:

P-3309912-166559

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

Yes

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.

No changes have occurred since the last PIA.

Describe the purpose of the system.

The National Institutes of Health (NIH) Enterprise Ethics System (NEES) is a secure web-based workflow management and information technology (IT) system that was developed to permit employees to electronically complete and submit their ethics requests and reports. The NEES allows for the submission, review, approval, and tracking of all ethics-related reports requests, and supporting personal financial data and documentation that are associated with the Ethics Program at NIH.

The system addresses consistency by enforcing standard routing and business rules for all employees who prepare and submit forms as well as for the ethics staff who review and approve the forms as well as a standard method for mapping data to the applicable form.

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

The system collects and maintains personally identifiable information (PII) and financial data for designated employees as well as their spouses and dependent children, including assets, income, liabilities, transactions, gifts, outside positions, and financial agreements. The system does not collect or store any identifying account numbers. Any financial documents containing identifying account numbers should be redacted by the individual uploading it or during the review process. Included within the personal financial data are the following PII: Name, email address, phone number, mailing address, entry-on-duty date, employment status, organization, salary, grade/step, position title, occupational series, financial disclosure status, appointment type and NIH user identification (ID). Additionally, some forms collect the name, organization, and title of a contact person from an outside employer or other entity. This information is either inputed directly by NEES users or downloaded from the NIH Enterprise Directory (NED) or Human Resources (HR) Database. NED and HR Database have their own and unique privacy impact assessments (PIAs) on records, with all legal authority documented. The NIH Ethics Officials (NEO) review information within NEES to ensure no actual or apparent conflict of interest exists that would breach the public trust.

Users log into this system using NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique PIA on record, including all legal authorities documented. The purpose of IAM Services 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. IAM Services collects unique user credentials and stores them in an encrypted format. IAM Services are an essential service which facilitates and governs network access to various resources.

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

NEES a secure web-based workflow management and IT system that was developed to permit employees to electronically complete and submit their ethics requests and reports. NEES allows for the submission, review, approval, and tracking of all ethics-related reports requests, and supporting personal financial data and documentation that are associated with the Ethics Program at NIH.

The system collects and maintains PII and financial data for designated employees, including assets, income, liabilities, transactions, gifts, outside positions, and financial agreements. The system does not collect or store any identifying account numbers. Included within the personal financial data are the following PII: Name, email address, phone number, mailing address, employment status, organization, salary, grade/step position title, financial disclosure status, appointment type and NIH user ID. This information is either inputted directly by NEES users or downloaded from the NIH NED and HR Database. NED and HR Database have their own and unique PIAs on records, with all legal authority documented. The NEOs review information within NEES to ensure no actual or apparent conflict of interest exists that would breach the public trust.

Users log in to this system using the NIH IAM Services which maintains its own unique PIA on record, including all legal authorities documented. The purpose of IAM Services 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. IAM Services collects unique user credentials and stores them in an encrypted format. IAM Services are an essential service which facilitates and governs network access to various resources.

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

Yes

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

Name
E-Mail Address
Mailing Address
Phone Numbers
Employment Status
Organization, entry-on-duty date, salary, grade/step, position title, occupational series, financial disclosure status, appointment type
Specific Financial Data (assets, liabilities, transactions, gifts, outside positions, and financial agreements)
NIH user ID

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

Employees
Public Citizens
Business Partner/Contacts (Federal/state/local agencies)

How many individuals' PII is in the system?

50,000-99,999

For what primary purpose is the PII used?

PII is used by ethics officials to review claims of misconduct or conflict of interests.

PII contained in NEES is shared with users in Department of Health and Human Services (HHS) Office of General Counsel (OGC) for the purpose of reviewing forms submitted by the senior staff at NIH.

The system collects authorized users' and administrators' user credentials (specified above) in order to control access to the system for the purpose of establishing use and viewing rights in the system.

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.

5U.S.C. 7301, 7351, 7353; 5 U.S.C. chapter 131 (Ethics in Government Act of 1978); 31 U.S.C. 1353; E.O. 12674 (as
modified by E.O. 12731); E.O. 13770 or any superseding Executive order; Representative Louise McIntosh
Slaughter Stop Trading on Congressional Knowledge Act (STOCK Act), Public Law 112–105 (2012), as amended; 5 CFR part 2634.

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.

OGE/GOVT-2, Executive Branch Confidential Financial Disclosure Reports.

OGE/GOVT-1, Executive Branch Personnel Public Financial Disclosure Reports and Other Name-

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Hardcopy

Online

Other

Government Sources

Within OpDiv

Other Federal Entities

Identify the OMB information collection approval number and expiration date

0209-0001, Expiration Date: 8/31/2027

0209-0006, Expiration Date: 8/31/2027

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Describe any agreements in place that authorizes the information sharing or disclosure.

Disclosure of information to other Federal agencies are made in accordance with federal laws and regulations as described in SORNs: OGE/GOVT-1 and OGE/GOVT-2, as well as internal procedures.

Describe the procedures for accounting for disclosures.

NEES maintains a robust auditing system for access to data. For each user log-in there are specific access limitations based on the user role such reviewer, certifier, auditor. Only users with permission may access limited data sets. Audit trail is maintained when any roles access the system data. Employees and direct contractors who maintain the system also have access to data, and but PII data is masked in development environments. All employees and contractor sign non-disclosures at the time of onboarding.

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

The NEES login screen has a privacy policy statement and notice which is presented upon logging into the NEES system. The notice informs individuals about their personal information and how it is used. NEES collects some limited data on system users/administrators (NIH staff) that have been given access rights to the system. Each individual gives personal information upon hiring. Notice of information collection is given at the time of acceptance of employment at the NIH.

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.

There is no option for opting-out. If system users/administrators do not wish to provide their user credentials in order to gain system access, they will be unable to do so.

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

Current system users are given notice via e-mail when major system changes occur. Former users are removed from the system.

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.

NIH staff can contact NED or HR Database directly since their PII is extracted from there.

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

NEES, in collaboration with the BAS Security Team, integrates analysis of audit records with the analysis of vulnerability scanning and system monitoring information to further enhance the ability to identify inappropriate or unusual activity. BAS Security team performs periodic scans of the system that include reviews of system vulnerabilities. NEES team participates in weekly BAS security meetings to discuss periodic reviews of system vulnerabilities and fix them based on their criticality. Employee data does get updated via cyclic Human Resources (HR) Database downloads.

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.

Determinations are made based on role-based access controls and least privilege. User rights are provisioned based on controls within the system, allowing users only access to the minimum amount of PII necessary to perform their job.

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 level to an individual's PII is dependent on system roles. The roles that enable access to anyone else's PII are assigned based on user need - the need to have access to information deemed necessary to perform the tasks associated with being an ethics reviewing official. In addition, an employee may voluntarily choose to designate someone as a NEES Assistant within the application. The Assistant would then be able to access PII within the individual's forms and application profile.

A NIH IAM Systems account login 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. Training is completed on the http://irtsectraining.nih.gov site with valid NIH credentials.

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

The NIH Ethics Office provides NEES training and reminds users of their responsibilities to protect PII and redact unnecessary PII included in documents within the system. All employees and contractors are also required to participate in annual online security awareness and privacy training that includes the fundamentals of protecting and handling PII within the agency.

In addition, all federal and contract employees must take mandatory Privacy and IT Security training annually.

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 following NIH Records Schedules:

Item: 06-801, General Ethics Program Records.
Description: Records created and maintained to coordinate and manage an agency's ethics program. Records relate to the development, review, implementation, and interpretation of proposed or established executive branch standards of ethical conduct and other ethics regulations; conflict of interest and other ethics-related statutes and Executive Orders; and any agency supplemental standards of ethical conduct and other agency ethics-related regulations and directives.
Disposition Instruction: Destroy 6 years following the conclusion of an ethics regulatory review, provision of advice to an employee, making a determination regarding outside employment or after such determination is no longer in effect or applicable, or when no longer needed for an active investigation; whichever is later, but longer retention is authorized if required for business use.
Disposition Authority: Disposition Authority Agency (DAA)-General Records Schedule (GRS)-2014-0005-0001

Item: 06-808, Public Financial Disclosure Reports. All other reports.
Description: Executive Branch, Personnel Public Financial Disclosure Reports (OGE Form 278) (formerly SF 278), OGE Form 278e, and related records.
Disposition Instruction: Destroy 6 years after receipt of the OGE Form 278 or 278e by the agency or when no longer needed for active investigation, whichever is later. This disposition instruction is mandatory; deviations are not allowed.
Disposition Authority: DAA-GRS-2014-0005-0008

Item: 06-812, Confidential Financial Disclosure Reports.
Description: Executive Branch Confidential Financial Disclosure Reports (OGE Form 450) and Confidential Certificates of No New Interests (OGE Optional Form 450- A), and related records.
Disposition Instruction: Destroy 6 years after receipt of the OGE Form 450 by the agency, except when the OGE Form 450 supports one or more subsequent Optional OGE Form 450-As then destroy 6 years after receipt of the last related OGE Form 450-A by the agency, or when no longer needed for active investigation, whichever is later. This disposition instruction is mandatory; deviations are not allowed.
Disposition Authority: DAA-GRS-2014-0005-0012

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

Physical Controls: The IT hardware used to host protected information is located in a secured datacenter facility. The facility is only open to authorized personnel whose access is monitored by locking doors with badge readers for both ingress and egress. Each discrete ingress and egress event is logged. The facility is under 24-hour surveillance by facilities security for security and environmental hazards.

Administrative Controls: All technical personnel who access IT systems which contain protected information have met background investigation criteria for Public Trust positions. All personnel have taken mandatory security and privacy training classes and annual refreshers. Administrative personnel accessing these systems use privileged and separate accounts for administrative access.

Technical Controls: IT hardware and software are segregated from default commodity public networks to prevent unauthorized or malicious access. Access controls lists and event logs are

maintained and monitored to detect unauthorized, suspicious or malicious activity. Access lists are restricted to approved IT technical personnel. Two factor authentication must be used for access. File integrity and auditing software are employed on hardware.