US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/12/2025

OPDIV:

NIH

Name:

NIH Enterprise Directory

PIA Unique Identifier:

P-4174780-432495

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

Conversion

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

The PIA has been updated to add additional details about the purpose in question 18, update question 11's purpose, and update the office in the point of contact information.

Describe the purpose of the system.

The NED system is a Major Application which services the entire NIH community by providing information about NIH Employees, Contractors, Fellows, Visiting Researchers, Foreign Nationals, Volunteers, Summer Students, Detailees, Tenants, and CIT Hosting Customers. NED provides workflow for NIH on-boarding and off-boarding business processes: Authorizes and deactivates all NIH staff’s access to NIH physical and logical resources (badge, network account, email, virtual private network (VPN), library, parking, etc.); Initiates required background investigation; Ensures continued management of essential processes for PIV badges and network accounts used to securely on-board new staff and promptly off-board terminated personnel and mitigate insider

threads and unauthorized access risk; Substantiates NIH staff in other critical HHS and NIH systems. NED is used by many Enterprise-wide systems, linked to institute and Center (IC) systems, and provides a internal interface to search for non-sensitive data about NIH staff.

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

The NED system is comprised of two separate components: NED Search (also known as NIH Staff Directory; ned.nih.gov) and the NED Portal (nedportal.nih.gov).

NED Search is an internet-based staff directory which allows access to work and locator information for NIH staff with full network access. NED Portal is an intranet site behind the NIH firewall which contains sensitive data.

Users of the NED web applications are responsible for the professional use of their accounts and user passwords as outlined in the NIH Rules of Behavior.

NIH Staff may view NED Search when logged through the NIH network. NED Search displays personally identifiable information (PII) including HHS identification (ID), legal name, work email, work location, mail stop code, work phone, work mobile phone, work facsimile transmission (FAX), IC, organization, classification, Intramural Position Designation (IPD), organizational title, pager number, teletypewriter (TTY), delivery address, postal address, website uniform resource locator (URL), NIH login username, NIH email, ID badge identifier, project officer, supervisor, servicing administrative officer (AO), and point of contact. NIH staff may opt out of sharing a work mobile phone and it will not be viewable.

The NED Portal contains additional PII and other sensitive data such as Social Security Number (SSN), date of birth (DOB), sex, place of birth, country of citizenship, residence address, home phone, mobile phone, permanent resident alien file number and ID photo. NED Portal also contains emergency contact information and includes the contact's full name, phone number and relationship.

The category of public citizens that may be in NED are emergency contacts, guest researchers, and volunteers. Emergency contacts are voluntarily entered by NIH Employees. Guest researchers and Volunteers' information is entered by the individuals themselves, or via the use of an official Office of Management and Budget (OMB) form which maintain their own current OMB Control Numbers.

NED Portal shares PII for a variety of reasons including personal identity verification, provisioning of NIH services, record matching, and in support of various NIH business processes. The NED Portal collects and maintains PII in the system database.

Additionally, the Center for Information Technology (CIT) IAM is responsible for the operation, maintenance, and support of NIH network accounts. Following authentication, individual NED record owners can view and update private information contained in their own record (Self Service Update) via a link on NED Search to a secure website which can only be accessed from within the NIH network.

Users log in to NED Portal using the NIH IAM Services which maintains its own unique privacy impact assessment (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. The IAM Services collect unique usernames and passwords (user credentials) and stores them in an encrypted format. The IAM Services are an essential service which facilitates and governs network access to various resources.

NED Portal also shares or discloses PII with several NIH and HHS systems as follows:
HHS Identity Management System (IDMS), NIH Background Investigation Tracking System (BITS), NIH IAM Services, NIH Web Services, NBIS/NIH Data Warehouse.
These systems maintain their own unique PIA, 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 NED system is a Major Application which services the entire NIH community by providing information about NIH Employees, Contractors, Fellows, Visiting Researchers, Foreign Nationals, Volunteers, Summer Students, Detailees, Tenants, and CIT Hosting Customers. NED provides workflow for NIH on-boarding and off-boarding business processes: Authorizes and deactivates all NIH staff's access to NIH physical and logical resources (badge, network account, email, VPN, library, parking, etc.); Initiates required background investigation; Ensures continued management of essential processes for PIV badges and network accounts used to securely on-board new staff and promptly off-board terminated personnel and mitigate insider threads and unauthorized access risk; Substantiates NIH staff in other critical HHS and NIH systems. NED is used by many Enterprise-wide systems, linked to institute and Center (IC) systems, and provides a internal interface to search for non-sensitive data about NIH staff.

NED Portal shares PII for appropriate business needs to support the NIH mission; including personal identity verification, provisioning of NIH services, record matching, and in support of various NIH business processes. The NED Portal collects and maintains PII in the system database. It also collects usernames (upon user login and authentication) and stores them as part of transaction/audit history and to provide authorization for access rights when users/administrators log into the portal.

Note: IDMS is part of another HHS system which has its own PIA - the HHS Identity and Access Management System (IAM@HHS). This system is owned by the Department of Health and Human Services, Office of the Secretary, Assistant Secretary for Administration, Office of Security and Strategic Information (HHS/OS/ASA/OSSI). NED and HHS@IAM have an Information Sharing Agreement (ISA).

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

Yes

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

Social Security Number
Date of Birth
Name
Photographic Identifiers
E-Mail Address
Mailing Address
Phone Numbers
Employment Status
Emergency contact and relationship, sex, place of birth, HHS ID badge identifier, mail stop code, FAX number, TTY, pager number
Home address, country of citizenship, permanent resident alien file number, web URL, emergency contact information, user names, employment status (classification),
Organizational affiliation, organizational title, IC, remote worker status; project officer, supervisor, servicing Administrative Officer (AO), point of contact, IPD

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

Employees
Public Citizens
Business Partner/Contacts (Federal/state/local agencies)
Volunteers, Guest Researchers, Fellows, Principal Investigators

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

The primary purpose of collecting PII is to support the administrative business processes which include, but are not limited to, the activation or creation of an HHS identification number and badge, initiating a background investigation, the establishment of an NIH network account, and the issuance of NIH parking permits. The NED system allows for the creation of accurate records for individuals in the NIH Directory.

Submission of personal information is required for the individual to obtain these services.

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

The secondary purpose of collecting PII is to provide services such as personal identity verification, provisioning of NIH services, record matching in support of various NIH business processes.

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

5 U.S.C. 301 and 302, 44 U.S.C. 3101 and 3102, and Executive Order 9397

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.

OPM/GOVT-1 General Personnel Records

09-25-0216 Administration: NIH Electronic Directory, HHS/NIH

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
Online
Other
Government Sources
Within OpDiv
Other HHS OpDiv

Identify the OMB information collection approval number and expiration date

0206-0182 - Declaration for Federal Employment (OF 306) Expiration Date: 8/31/2026

1615-0047 Employment Eligibility Verification - Expiration Date: 7/31/2026

0925-0001 Public Health Service (PHS) Applications and Pre-award Related Reporting (OD) - Expiration Date: 1/31/2026

0925-0002 PHS Research Performance Progress Report and Other Post-award Reporting (OD) - Expiration Date: 1/31/2026

0925-0670 NIH Information Collection Forms to Support Genomic Data Sharing for Research Purposes (OD)- Expiration Date: 03/31/2026

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.

NED business owners have an Information Sharing Agreement (ISA) with the HHS Office of the Secretary for the HHS Identity and Access Management System (IDMS/IAM@HHS).

This system is tied to the provisioning, management, and identity of NED accounts.

Describe the procedures for accounting for disclosures.

By default, organizations do not have access to NED sensitive data. However, HHS and NIH organizations can request access to sensitive data from NED by filling out a NED Privacy Act Data Request Form. The requester must sign the form to indicate agreement. The completed form is submitted to and approved by the CIT Privacy Coordinator and kept on file by the NED Program. Access to NED sensitive data is set up, controlled, and monitored by the NED team. Access is granted only after CIT Privacy Coordinator approval.

Additionally, ISAs identify and track specific sensitive data elements which NED provides to other systems.

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 HHS IDMS has its own PIA and its own process for notifying individuals their information will be collected.

The NED user interface displays the following message to record-owners or administrative staff at the time a person is registered in NED and when an NIH employee (federal or direct contractor) modifies their information already in NED:

PRIVACY ACT NOTIFICATION STATEMENT
Collection of this information is authorized under 5 U.S.C. 301 and 302, 44 U.S.C. 3101 and 3102, and Executive Order 9397. The primary use of the information you provide is to enter the data into the NIH Enterprise Directory (NED) in order that NIH centrally support administrative business processes which include, but are not limited to, the activation or creation of an NIH identification number, the establishment of an e-mail account on the NIH network or the issuance of an NIH parking permit. The NED system allows for the creation of accurate records for individuals in the NIH Directory. Typical users of this information will be Trans-NIH Human Resource Specialists, Administrative Officers/Technicians, Contractors, Project Managers, Information Resources Management staff, Space and Facility Management personnel, Supervisors, Information Systems Security Officers and other NIH Central Services Staff. For further information as to how the information you provide may be disclosed, please refer to the NIH Privacy Act Systems of Records Notice which covers the information collection. It is entitled #09-25-0216 "Administration: NIH Electronic Directory, HHS/NIH" and is available at URL: https://www.hhs.gov/foia/privacy/sorns/nih-sorns.html Submission of this information is voluntary, however, in order for us to activate or create an NIH ID for you to visit our campus, create an e-mail account and issue an NIH parking permit, you should complete all fields.

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.

Individuals have the option to withhold their PII during the registration process. However, refusal makes it difficult for a person to carry out his/her official NIH duties and responsibilities since registration in NED is a prerequisite for obtaining NIH services, including logical access to information systems/email and physical access to facilities, parking, NIH Library access, and listings in the NIH Telephone and Services Directory.

Users have the option to enter their own PII during the registration process. NIH administrative staff has the option of requesting an individual enter their PII directly into NED and the individual must agree to the following prior to submission:

"I hereby authorize the release of information in this application to appropriate Federal agencies for the purposes of processing this application and verifying my identity. I also acknowledge that if I provide or assist in the provision of false information or non-verifiable information, and/or I purposely omit information, it could result in loss of access to HHS facilities and IT systems and in disciplinary action including removal from Federal service or a Federal contract, and I may be subject to prosecution under applicable Federal criminal and civil statutes. I declare under penalty of perjury that the foregoing is true and correct."

When NIH administrative staff enters an individual's PII, they must certify the information is entered using information from Section A of a completed HHS-745 ID Badge Request form that was signed by the individual.

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

Individuals have the option to withhold their PII during the registration process.

There are no other processes in place to obtain additional consent from the individuals whose PII is stored in NED regarding what PII is collected for them or how the information will be used or shared. There are also no processes in place to obtain consent from the individuals whose PII is in the system when major changes occur to the system. In the event NED changes the way its data is used or disclosed, an appropriate option for notifying individuals and obtaining their consent may be employed (based on technical and business process considerations).

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 the NIH IT Service Desk and if necessary, a ticket is assigned to the NED operations and support team for action. Individuals may also contact the NED team directly at nedteam@mail.nih.gov.

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

The PII is reviewed when HHS Personal Identity Verification (PIV) cards (badges) are renewed. The timeline for badge renewal depends upon the type of badge and typically ranges from one (1) year to five (5) years. Alternatively, individuals have the option to conduct reviews of their own PII through NED Self Service.

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.

All NED development team and management team staff have appropriate position sensitivity levels. Background investigations are conducted according to their assigned position.

Core users of the main NED web application include users with the AO or AT role. NED IC Coordinators or existing AO users grant, modify, and remove AO and AT access using functionality in the NED Portal. NED system administrators authorize people for other system roles upon request by an authorized NIH business owner.

NED staff manages the Oracle database accounts used by systems that access NED data stored in the Oracle database. The CIT Privacy Coordinator must authorize access to private data covered under the NED System of Records Notice (SORN). Downstream applications using sensitive NED Oracle data include HHS IDMS, NIH BITS, NIH IAM Services, NIH Web Services, NBIS/NIH Data Warehouse, IAM Virtual Directory Services (VDS).

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 other than a person's own information is restricted to administrative staff in their direct organization. Other access is on a need to know basis, with specific data field access based on application needs.

AO and AT maximum scope of authority is limited to records affiliated with their own IC and may be further restricted to records affiliated with specific organizations in the IC. NED automatically removes the user access (including AOs and ATs) when their NED record is deactivated or transferred to a different IC. Authentication to NED is via NIH IAM Services.

CIT is responsible for the operation, maintenance, and support of NIH IAM accounts. Following NIH login authentication, NED record owners can view private information contained in their own record via a secure website from a computer attached to NIHnet.

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.

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).

Training is offered monthly and is mandatory for all new AO/AT users and every three (3) years thereafter.

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 10-101 - Administrative records maintained in any agency office.
Administrative records maintained in any agency office. Records accumulated by individual offices that relate to routine day-to-day administration and management of the office rather than the mission-specific activities for which the office exists, excluding records scheduled elsewhere in the General Records Schedule (GRS) such as timekeeping and procurement.
Disposition: Destroy when business use ceases. DAA-GRS-2016-0016-0001

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

Administrative:
NED maintains administrative controls and is assessed by the NIH Security Assessment & Authorization Program and granted an Authorization to Operate (ATO) by NED's Authorizing Official. System Security, Contingency, and Configuration Management Plans exist and are reviewed and updated annually or upon changes to the system.

Mandatory NED training classes are offered once a month for new AOs/ATs and existing AOs/ATs who are required to take NED refresher training every three (3) years. The NED team also maintains a NED Administrator Guide which includes all essential information and is updated to reflect changes as needed.

Access to other than a person's own information is restricted to administrative staff in their direct organization. Other access is on a need to know basis, with specific data field access based on application needs. Additionally, contractors who work on the system are required to sign NIH Non-Disclosure Agreements.

NED has a configuration management process whereby all system code is maintained under change control. All proposed changes are reviewed by a team for operational and security impact, coded, unit tested in development, and regression tested in a test environment. Once testing has been completed and a rollback plan created, approval to move to production is given.

Technical:
Technical Controls minimize the possibility of unauthorized access, use or dissemination of the data in the system. NED utilizes the NIH computer network (NIHnet) operated by CIT's Division of Network Systems and Telecommunications. Other technical controls include regular file back-ups, user identification, passwords, firewall, VPN, encryption, intrusion detection system (IDS), smart cards and public key infrastructure (PKI). A process exists to monitor and respond to security incidents. The NIH Incident Response Team (IRT) maintains the NIH Incident Handling Procedures which outlines how to handle, report, and track incidents and/or problems. The procedures describe the roles of the IRT and Information System Security Officer (ISSO). The IRT has a 24 x 7 contact number available to ISSOs (301-881-9726) and can be reached at IRT@nih.gov.

Physical:
Physical access controls include guards, identification badges, key cards, and closed-circuit TV (CCTV). NED physical, network and operating system security controls are maintained by CIT.

Note: web address is a hyperlink.