US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/10/2025

OPDIV:

NIH

Name:

OD General Support System

PIA Unique Identifier:

P-2198938-824928

The subject of this PIA is which of the following?

General Support System (GSS)

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

Internal Flow or Collection

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

Since the last Privacy Impact Assessment, the The Office of the Director (OD) General Support System (GSS) has been expanded to include the following non-sensitive personally identifiable information: name, email, mailing address, phone number, and organizational affiliation.

Describe the purpose of the system.

The Office of the Director (OD) General Support System (GSS) supports information technology-based services that are used to further the mission of the OD. The OD GSS is comprised of information technology equipment, including, but not limited to, network monitoring tools and devices, security monitoring tools and devices, desktop and laptop computers, network and archive storage, and equipment and software necessary to support application hosting.

The OD maintains a list of sub-systems and applications in the Department of Justice's Governance, Risk, and Compliance system, Cyber Security Assessment and Management Application. Additionally, each sub-system and application maintains their own privacy risk assessment.

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

As a GSS, the OD GSS only contains minimal, non-sensitive personally identifiable information (PII). The PII is limited to for contact information or name, email, mailing address, phone number, and organizational affiliation. There are only two use cases for this PII:

When collecting data that is derived from a "Contact us" type of form, such as those on a public facing website, or -

As an electronic directory supporting e-government and administrative business processes at NIH.

The OD GSS contains significant subcomponents (subsystems and applications) which are essential to achieving the mission of the OD. These subsystems have unique and specific Privacy Impact Assessments (PIAs) which address the type of information the specific system will collect, maintain, store, and share, including personally identifiable information (PII). Each subsystem will list the OD GSS' Universally Unique Identifier (UUID) within their respective PIAs.

Users log in to the various supported systems using the NIH Identity, Credential, and Access Management (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 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.

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

The Office of the Director (OD) General Support System (GSS) supports information technology-based services that are used to further the mission of the OD. The OD GSS is comprised of information technology equipment, including, but not limited to, network monitoring tools and devices, security monitoring tools and devices, desktop and laptop computers, network and archive storage, and equipment and software necessary to support application hosting.

The OD maintains a list of sub-systems and applications in the Department of Justice's Governance, Risk, and Compliance system, Cyber Security Assessment and Management Application. Additionally, each sub-system and application maintains their own privacy risk assessment.

As a GSS, the OD GSS only contains minimal, non-sensitive personally identifiable information (PII). The PII is limited to for contact information or name, email, mailing address, phone number, and organizational affiliation. There are only two use cases for this PII:

When collecting data that is derived from a "Contact us" type of form, such as those on a public facing website, or -

As an electronic directory supporting e-government and administrative business processes at NIH.

The OD GSS contains significant subcomponents (subsystems and applications) which are essential to achieving the mission of the OD. These subsystems have unique and specific Privacy Impact Assessments (PIAs) which address the type of information the specific system will collect, maintain, store, and share, including personally identifiable information (PII). Each subsystem will list the OD GSS' Universally Unique Identifier (UUID) within their respective PIAs.

Users log in to the various supported systems using the NIH Identity, Credential, and Access Management (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 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.

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
organizational affiliation

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

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

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

As an electronic directory supporting e-government and administrative business processes at NIH.

Or, to communicate OD initiatives with individuals requesting more information about NIH.

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

NA

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

42 U.S. Code § 281, 5 U.S.C. 301, 305, 553; 21 U.S.C. 301 et seq.; 31 U.S.C. 1115(b)(6); 40 U.S.C. 11313; 42 U.S.C. 201 et seq.; 44 U.S.C. 3101, 1505; E.O. 11583; E.O. 13571.

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.

09-90-1901, HHS Correspondence, Comment, Customer Service, and Contact List Records

09-25-0216 Administration: NIH Electronic Directory

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Email

Online

Government Sources

Within the OPDIV

Other HHS OPDIV

State/Local/Tribal

Other Federal Agencies

Non-Government Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

N/A. As an electronic directory serving administrative processes, the information is that of employees. For contact information, the Office of Management and Budget (OMB) does not require an OMB clearance.

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.

For contact information, individuals are directed to the NIH Privacy Policy/Notice which includes a statement that personally identifiable information (PII) is optional and is collected voluntarily.

For internal use, employees are notified during the on-boarding process that their contact information and picture are available in a directory. They may contact Human Resources (HR) if they need assistance.

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.

As a contact for more information, users can decline to provide PII. However, without their contact information there is no way to respond directly.

As a electronic directory supporting e-government and administrative business processes, the information is obtained from NED, the source system and maintains its own PIA.

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

There will be no substantive changes to data uses. Information is collected in order to respond to requesters. There is no further use of PII. In the event of a major change, the email address will be used to contact individuals.

As an electronic directory supporting e-government and administrative business processes, the information is obtained from NED, the source system and 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.

If an individual chooses to include personal information, it is voluntary. Should concerns arise or a need to update information, users could access the contact us page of the site or the NIH Privacy Office at Privacy@mail.nih.gov.

As an electronic directory supporting e-government and administrative business processes, the information is obtained from NED, the source system and maintains its own PIA.

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 NIH information technology (IT) Privacy Program requires systems to implement privacy reviews and controls throughout the development life cycle, and to incorporate review of privacy controls into the annual assessment schedule of controls on all systems, networks and interconnected systems.

Regular security, 'health checks' and backups are completed, and vulnerabilities are addressed. PII is generally collected as a one-time use in a request for additional information on a particular topic or application.

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.

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.

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).

NA

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 11-102 - Public Correspondence and Communications not Requiring Formal Action.
Records related to correspondence and communications, including comments, to and from the public that require no formal response or action.
Disposition: Destroy when 90 days old, but longer retention is authorized if required for business use. DAA-GRS-2016-0005-0002

Item 07-203 - System access records. Systems not requiring special accountability for access. These records are created as part of the user identification and authorization process to gain access to systems. Records are used to monitor inappropriate systems access by users.
Disposition: Destroy when business use ceases. DAA-GRS-2013-0006-0003

12-039 - Administration: NIH Enterprise Directory (HHS/NIH)
This system allows for the creation of accurate records for individuals in the NIH directory and ensures that duplicate data files are compared, corrected, and combined for accuracy, thus, eliminating redundancy. It is the central point of coordination for other automated systems that manage or track resources, particularly information security systems.
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 controls include system security and contingency plans. Files are backed up regularly. 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 sites use privileged and separate accounts for administrative access.

Technical controls include User identification (ID), passwords, network firewall, Virtual Private Network (VPN), Intrusion Detection System, Role Based Access Controls, System logs. IT hardware and software is 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 authentications must be used for access. File integrity and auditing software are employed on hardware.

Physical controls may include 24x7 guards, secure building access, Personal Identify Verification (PIV) card access and/or closed-circuit television (TV). The IT hardware used to host protected information is located in a secured data center 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.