US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

08/26/2025

OPDIV:

NIH

Name:

Custom-Developed Apps (CDA)

PIA Unique Identifier:

P-7715313-921956

The subject of this PIA is which of the following?

Minor Application (child)

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?

Yes

Identify the operator.

Agency

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

Yes

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

Describe the purpose of the system.

The Custom-Developed Apps (CDA) is a subsystem of the Office of Research Services (ORS) and Office of Research Facilities Development and Operations (ORF) General Environment Moderate (OGEM) that have several components residing on the Enterprise Network Services (ENS). These components are software applications designed and built by the Office of Innovation and Information Technology (OIIT) Software Development Services (SDS) team based on business needs of the ORS and ORF community. CDA applications are used by ORS-ORF staff to process requests to provide administrative and research services.

The components that provide administrative services are:

-Commuting and Parking Services (CAPS) to request parking, carpool and transhare.
-Confined Space to outline procedures to be followed when accessing confined spaces within NIH.
-Division of Fire Marshall (DFM) to report fire safety complaints, fire code violations or fire safety issues

-Division of Medical Arts (DMA) Events requests to request facilities and services for NIH mission-related activities.
-DVR Billing System (DVRBS) to collect billing data and submit to NIH Business System (NBS).
-Emergency TERMS (not an acronym) to track conference attendance of members.
-Mail Stop Code (MSC) Admin to track and report courier pickup and delivery calls on the NIH campus and satellite offices.
-Medical Arts Branch (MAB) Commerce to request medical art services

The components that provide research related services are:

-Animal Transport Request (ATR) to track transportation of animals and various species within NIH.
-Division of Veterinary Resources Technical Service Request Application System (DVR TSRAS) to request technical services be performed, such as special tests, to the animal species.
-Division of Veterinary Resources (DVR) Web Health (Web Health) to request diagnostic tests to the animal species.
-Electronic Registration System (ERS) to track exposure information to pathogens, either human or non-human primate (NHP) species.
-NIH Online Rodent Import Application System (NIH ORIAS) to request and track rodent tests performed.
-NIH Visiting Scientists Tracking Automation System (NVISTAS) to request immigration-related services to foreign scientist research community.

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

The system collects, maintains, and shares information necessary for providing several services across the NIH campus and its satellite offices. All components collect Personally Identifiable Information (PII) to identify requesters and provide the service requested, and at a minimum include contact information (name, email address and phone number). In addition, components collect specifically:

-CAPS: photo, license plate, mailing address, employment status, Personal Identify Verification (PIV) Identification (ID) number, badge expiration date, Institute, Centers and Offices (ICO), Building, Room, Organizational Unit.
-Confined Space: campus, building, floor, room and space type.
-DFM: request date and location (area/building/room number).
-DMA Events: Institute, Center, or Office (ICO), Common Accounting Number (CAN), Event Date.
-DVRBS: ICO, CAN.
-Emergency TERMS: unit, shift, drill type, date/time.
- MSC Admin: username and password.
-MAB: request date, ICO and Common Accounting Number (CAN)
-ATR: ICO, building, room.
-DVR TSRAS: Campus, ICO, Building, Room, CAN.
-DVR Web Health: Campus, ICO, Building, Room, CAN.
-ERS: PIV Card Number, ICO, Date, Campus, Building, Room.
-NIH ORIAS: mailing address, Campus, ICO, room, fax number, date of arrival.
-NVISTAS: Social Security Number (SSN), date of birth (DOB), photo, mailing address, legal documents, education records, employment status, foreign activities, passport and visa numbers and Curriculum Vitae (CV).

NIH employees log into the system 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 CDA is a subsystem of OGEM that has several components residing on the ENS. These components are software applications designed and built by the OIIT SDS team based on business needs of the ORS and ORF community. CDA applications are used by ORS-ORF staff to process requests to provide administrative and research services. The components that provide administrative services are:

-CAPS to request parking, carpool and transhare.
-Confined Space to outline procedures to be followed when accessing confined spaces within NIH.
-DFM to report fire safety complaints, fire code violations or fire safety issues
-DMA Events requests to request facilities and services for NIH mission-related activities.
-DVRBS to collect billing data and submit to NBS.
-Emergency TERMS to track conference attendance of members
- MSC Admin to track and report courier pickup and delivery calls on the NIH campus and satellite offices.
-MAB Commerce to request medical art services

The components that provide research related services are:
-ATR to track transportation of animals and various species within NIH.
-DVRTSRAS to request technical services be performed, such as special tests, to the animal species.
-DVR Web Health to request diagnostic tests to the animal species.
-ERS to track exposure information to pathogens, either human or NHP species.
-NIH ORIAS to request and track rodent tests performed.
-NVISTAS to request immigration-related services to foreign scientist research community.

The system collects, maintains, and shares information necessary for providing several services across the NIH campus and its satellite offices. All components collect PII to identify requester and provide the service requested, and at a minimum include contact information (name, email address and phone number). In addition, components collect specifically:
-CAPS: photo, license plate, mailing address, employment status, PIV ID number, badge expiration date, ICO, Building, Room, Organizational Unit.
-Confined Space: campus, building, floor, room and space type.
-DFM: request date and location (area/building/room number).
-DMA Events: ICO, CAN, Event Date.
-DVRBS: ICO, CAN.
-Emergency TERMS: unit, shift, drill type, date/time.
- MSC Admin: username and password.
-MAB: request date, ICO and Common Accounting Number (CAN)
-ATR: ICO, building, room.
-DVR TSRAS: Campus, ICO, Building, Room, CAN.
-DVR Web Health: Campus, ICO, Building, Room, CAN.
-ERS: PIV Card#, ICO, Date, Campus, Building, Room.
-NIH ORIAS: mailing address, Campus, ICO, room, fax number, date of arrival.
-NVISTAS: SSN, DOB, photo, mailing address, legal documents, education records, employment status, foreign activities, passport and visa numbers and CV.

NIH employees log into the 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. 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.

Social Security Number
Date of Birth
Name
Photographic Identifiers
Vehicle Identifiers
E-Mail Address
Mailing Address
Financial Accounts Info
Legal Documents
Education Records
Employment Status
Foreign Activities
Passport Number
Taxpayer ID
License plate, Badge expiration date
PIV ID number, username and password, CV
ICO, Campus, Building name, Floor number, Room number, Organizational unit, Space type
Request date, Date of arrival, Inspection date, Event date
Fax number, CAN and Task number

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
Patients

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

To identify requester and provide the service requested.

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

There are no secondary uses.

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

U.S.C. 301, 302; 42 U.S.C. 203, 282; 44 U.S.C. 3101; E.O. 10450

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.

09-25-0140, International Activities: International Scientific Researchers in Intramural Laboratories at

09-25-0167, National Institutes of Health (NIH) TRANSHARE Program, HHS/NIH/OD

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

Government Sources

Within the OD

Identify the OMB information collection approval number and expiration date

An OMB information collection approval is not required for federal employees. Information that is collected from public citizens on DMA, MAB and NVISTAS, is exempt because the information is used solely to self identify and request services.

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.

There is an overarching MOU and ISA in place, that the system inherits. The parties include between NIH OD/ORS/ORF and Center for Information Technology, Business Application Services (CIT/BAS) NIH Enterprise Directory System (NED); between NIH Business System (NBS) Office of Director (OD) and
Division of Veterinary Resources (DVR) Billing System Office of Research Services (ORS).

Describe the procedures for accounting for disclosures.

They will be developed with Privacy Coordinator guidance.

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 NVISTAS Foreign Nationals are notified their personal information will be collected via the 829-1 and 829-2 forms have a privacy statement that their information will be collected they submit to NIH.

All other components do not provide written notification that the PII will be collected, but it is self-explanatory as the individual is completing the request.

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 opt-out option; individuals can choose to not enter their information but then will not be able to complete their request.

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

When a major change occurs to the system that affect the use or disclosure of PII, the organization updates the Privacy Impact Assessment and/or SORN as required, notifies affected individuals through appropriate channels (e.g., email, mail, or system notice), and obtains their consent when necessary; if notification or consent is not feasible, a documented justification is provided explaining the reasons and outlining measures to protect the data.

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 program managers (administrators) who will contact the ORF Privacy Coordinator and/or System Owner for resolution.

Individuals may also contact the NIH Privacy Office at Privacy@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 NIH IT Privacy Program requires system owners 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.

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.

System administrators are approved based on their technical/functional role in administering, developing, and supporting the daily job functions of the system.

nVISTAS contains built in user levels managed by the system owner. Determinations conform to 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.

For other components, users will be able to view/edit all 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. Administrators and Privileged Users require additional training specific to their roles and responsibilities.

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

IT Specialist (SYSADMIN) users are required to do annual and on point of entry role-based training.

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.

Item 09-201: Facility, space, vehicle, equipment, stock, and supply administrative and operational records. Records relating to administering and operating facilities, spaces, Federally owned and operated housing, land vehicles, water vessels, equipment, stocks, and supplies.
Destroy when 3 years old or 3 years after superseded or obsolete, whichever is applicable. Longer retention is authorized for business use. DAA-GRS-2016-0011-0001
Item 09-207: Facility, space, and equipment inspection, maintenance, and service records. Records tracking completion of custodial and minor repair work.
Destroy when 90 days old, but longer retention is authorized if required for business use. DAA-GRS-2016-0011-0009

Item 09-302: Mail, printing, and telecommunication services administrative and operational records. Records of internal mail room, printing/duplication services, and radio/telecommunication services administration and operation.
Mail, printing, and telecommunication services administrative and operational records. Records of internal mail room, printing/duplication services, and radio/telecommunication services administration and operation.
Destroy when 3 years old, or 3 years after applicable agreement expires or is cancelled, as appropriate, but longer retention is authorized if required for business use. DAA-GRS-2016-0012-0001

Item 04-201:Animal Husbandry Records
NIH animal husbandry and veterinary services records document NIH's laboratory animal support programs, as they seek to contribute to the advancement of the NIH biomedical research mission. Animal husbandry records are associated with animal caretaking activities, and animal facility management. Veterinary services records are associated with veterinary procedures and activities, animal health and welfare records, animal study information that support research endeavors.
Destroy when 3 years old unless records directly relate to a protocol, in which case destroy 3 years after the end of the relevant activities. Longer retention is authorized if required for business use. DAA-0443-2018-0003-0001

Item 06-118: Special hiring authority program records
Special hiring authority program records. Records an agency creates and receives that document its administration of special hiring authority programs such as summer, student, intern, and other temporary hiring authorized by OPM.
Destroy 2 years after hiring authority closes but longer retention is authorized if required for business use. DAA-GRS-2014-0002-0016

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

Administrative Controls: All technical personnel who access IT systems which contain protected information have met background investigation criteria for Public Trust positions.

Physical Controls: The information technology (IT) hardware used to host protected information is located in a secured room within the DP facilities. This room is only open to authorized personnel whose access is monitored by locking doors with badge readers, which logs the access event. The facility is under 24-hour surveillance by facilities security for security and environmental hazards.

Technical Controls: IT hardware and software is segregated from default commodity public and NIH networks to prevent unauthorized or malicious access. Access controls lists and event logs are maintained and monitored locally to detect unauthorized, suspicious or malicious activity. Access lists are restricted to approved IT technical personnel and managed by the system Administrator.

The users/administrator will require an independently established username/password to access the system. These system and application login accounts are managed by the System Owner and Technical Administrator to control and limit user access.

Identify the publicly-available URL:

https://orderonline.medarts.nih.gov/
https://orsapps.od.nih.gov/DMA/DMAEventRequest/DMA_EventRegister.aspx
Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Does the website have any information or pages directed at children uner the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

No

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

null