US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

09/09/2025

OPDIV:

NIH

Name:

DOHS-CERTS

PIA Unique Identifier:

P-8359553-679530

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 and update the status of the Division of Occupational Health and Safety (DOHS) Certification (CERTS)

Describe the purpose of the system.

The Division of Occupational Health and Safety (DOHS) Certification (CERTS) database stores equipment certification, installation, maintenance and decontamination records. Examples of equipment included in the DOHS-CERTS database are biological safety cabinets, animal care modules, chemical fume hoods, local exhaust ventilation devices (LEVs), and all high efficiency particulate air (HEPA) filtered equipment. In addition, records are stored for other types of primary barrier equipment, such as, vertical and horizontal clean benches, cage change stations, animal racks, animal isolators, and heating, ventilation and air conditioning (HVAC) HEPA filter banks.

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

DOHS-CERTS collects contact's name, phone number, building, room number, email, and institute, center or office (ICO). In addition, DOHS personnel and contract staff working in the field use wireless tablets to enter equipment certification and maintenance information into reports on the DOHS-CERTS application. The information recorded on the tablets is synced through a hard Ethernet connection, so authentication is through a NIH secure service account.

The DOHS-CERTS users log in to this system using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (PIA) on record, with 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.

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

The DOHS-CERTS database stores equipment certification, installation, maintenance and decontamination records. Examples of equipment included in the CERTS database are biological safety cabinets, animal care modules, chemical fume hoods, LEVs, and all HEPA filtered equipment. In addition, records are stored for other types of primary barrier equipment, such as, vertical and horizontal clean benches, cage change stations, animal racks, animal isolators, and HVAC HEPA filter banks.

The only PII the lab technician collects: contact's name, phone number, building, room number, email, and ICO. In addition, DOHS personnel and contract staff working in the field use wireless tablets to enter equipment certification and maintenance information into reports on the DOHS-CERTS application. The information recorded on the tablets is synced through a hard Ethernet connection, so authentication is through a NIH secure service account.

The DOHS-CERTS users log in to this system using the NIH IAM Services which maintains its own unique PIA on record, with 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 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
Building, room number
ICO

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

Employees
Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

The primary purpose of the PII is to associate a requester with a service request created for maintenance and repair of equipment.

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

The DOHS–CERTS uses reporting capabilities for survey and regulatory compliance purposes.

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

5 USC 301 and 302, 44 USC 3101 and 3102, 44 USC 2904 and 2906

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.

SORN: 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
Email
Online
Government Sources
Within OpDiv
Other HHS OpDiv
Other Federal Entities
Non-Governmental Sources
Private Sector

Identify the OMB information collection approval number and expiration date

Not Applicable; an OMB collection approval number is not required as the DOHS-CERTS is not conducting or soliciting information.

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.

No formal agreements exist. However, since the NIH is a regulated entity we must comply with federal regulations and provide information when necessary, or as is described in the applicable Code of Federal Regulations (CFR).

Describe the procedures for accounting for disclosures.

The application System Owner, after receipt of a written request, will review the system to

verify that the requested record exists. No disclosure takes place without verification of the requester's identity.

Verification of identity is established by providing either a notarized request or both a written certification of identity and a statement of understanding that a knowing and willful request for the acquisition of a record under false pretenses is a criminal offense.

Information is sanitized and PII is either removed or redacted before disclosure unless required by regulation

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 website is hosted in the ORS Application Hosting Environment (AHE) and the NIH Privacy notice is provided to all visitors logging in to the website.

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 individuals to opt-out of the collection of use of their PII as the information collection is required for the work-flow and to process requests.

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

Individuals are notified of major changes that occur in the NIH NED through official notices sent out or when an Administrative Officer updates or changes PII within 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.

If an individual has concerns that their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate, they may contact the POC in question 6.

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 DOHS–CERTS goes through the annual Information Technology Security Assessment & Authorization (SA&A) and Privacy Impact Assessment (PIA).

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 based on role of person and the need to use or have access to the system. All requests for access go through the system administrator.

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.

Appropriate access is granted to the system based on predefined roles and job descriptions, and administrative access is limited to authorized employees based on current roles. Authentication with NIH Personal Identity Verification (PIV) card will occur at time of login to the NIH Network.

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).

No training above and beyond general security and privacy awareness training required.

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: 06-704.
Description: Workplace environmental monitoring and exposure records. OSHA-regulated substance monitoring and exposure records.
Results or measurements of monitoring workplace air, toxic substances, or harmful physical agents, including personal, area, grab, wipe, or other methods of sampling results.

Area/general occupational exposure records and select carcinogen exposure records from hazardous chemical use in laboratories. Includes the Chemical Hygiene Plan.

Exclusion: Employee-specific occupational exposure records appropriate for individual occupational medical case files are covered by RSS Item 06-709 (GRS 2.7, Item 060).
Legal Citations: 29 CFR Part 1910.1020(d)(1)(ii) and 29 CFR Part 1910.1020(d)(1)(iii)
Note 1: Biological monitoring results, such as blood and urine analysis results, designated as exposure records by specific Occupational Safety and Health Administration (OSHA) standards are maintained as required by the specific standard governing their use. For more information, refer to 29 CFR 1910.1020(c)(5) – Employee exposure records and 29 CFR 1910.1020(c)(5)(ii).
Note 2: These items are intended for agencies subject to Executive Order 12196, Occupational Safety and Health Programs for Federal Employees. Entities excluded from these requirements may use these items or agency-specific schedules.

Disposition: Destroy no sooner than 30 years after monitoring is conducted, but longer retention is authorized if needed for business use.

Disposition Authority Agency: DAA-GRS-2017-0010-0004

Item Number: 07-201

Description: Systems and data security records.
These are records related to maintaining the security of information technology (IT) systems and data.
Records outline official procedures for securing and maintaining IT infrastructure and relate to the specific

systems for which they were written. This series also includes analysis of security policies, processes, and
guidelines, as well as system risk management and vulnerability analyses. Includes records such as:
• System Security Plans
• Disaster Recovery Plans
• Continuity of Operations Plans
• published computer technical manuals and guides
• examples and references used to produce guidelines covering security issues related to specific systems
and equipment
• records on disaster exercises and resulting evaluations
• network vulnerability assessments
• risk surveys
• service test plans
• test files and data

Disposition Instruction: Destroy 1 year(s) after system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system.

Disposition Authority: DAA-GRS-2013-0006-0001

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. 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.

Physical Controls: The information technology (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.

Technical Controls: 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 authentication must be used for access. File integrity and auditing software are employed on hardware.