US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

09/25/2025

OPDIV:

NIH

Name:

ORS DOHS Integrated Pest Management System (IPMS)

PIA Unique Identifier:

P-1303640-684947

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?

No

Identify the operator.

Contractor

Is this a new or existing system?

Existing

Does the system have Security Authorization (SA)?

No

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

PIA Validation

Significant System Management Change

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

The system has a new planned Security Authorization date and is now residing behind the NIH firewall. No other changes were made.

Describe the purpose of the system.

The Integrated Pest Management System (IPMS) is a data repository and reports development and distribution system. It tracks the Integrated Pest Management services provided at National Institutes of Health (NIH) facilities. It also provides data storage, tracking incidents and surveys of the Food Safety Programs. As well as recording the completion of personnel IPMS training and development of certificates.

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

The following Personally Identifiable Information (PII) is maintained in the system: names, emails,

phone numbers, certificates, mailing addresses (building and room numbers).

Users log into the system with a username and password unique to each individual.

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

The IPMS is a data repository and reports development and distribution system. It tracks the Integrated Pest Management services provided at NIH facilities. It also provides data storage, tracking incidents and surveys of the Food Safety Programs. As well as recording the completion of personnel IPMS training and development of certificates.

The following PII is maintained in the system: names, emails, phone numbers, certificates, mailing addresses (building and room numbers).

Users log into the system with a username and password unique to each individual.

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
Certificates
Username and password

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 send out reports to those who have authority and responsibility to assist as a liaison in the Integrated Pest Management Program (IPMP).

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

A paper sign-up sheet is used at Integrated Pest Management training to educate about structural, behavioral, sanitation and pest biology at each facility. Names are collected to generate a certificate of completion for any training.

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

Title 7 U.S.C. Section 136r-1, 42 U.S.C. 241, 5 U.S.C. 7902

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.

09-25-0166 Administration: Radiation and Occupational Safety and Health Management Information

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Email

Online

Government Sources

Within the OPDIV

Identify the OMB information collection approval number and expiration date

Non-applicable, an OMB collection approval number is not required as IPMS is not surveying or soliciting information. The system only stores the names of attendees regarding various training to generate certificates for attendees.

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.

Only NIH employees, information technology (IT) developers, technicians, and direct contractors have access to the system which shows the terms of use and NIH Privacy Statement at the bottom of the log in page.

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 for individuals. Individuals not wishing to provide their information can choose not to. However, participation in the program or to work for NIH requires such information. Failure to submit PII would terminate the requester's application.

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

Group or individual email notifications are written and sent through the Administrator function to notify and obtain consent from the individuals whose PII is in the system when major changes occur in 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.

An individual may email the system administrator at lubbertt@nih.gov with concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. Issues can be resolved and inaccurate information corrected through the Administrator function.

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

IPMS goes through the annual Information Technology Security Assessment & Authorization (SA&A). Reviews of privacy controls are part of the annual assessment schedule.

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 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.

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 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.

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).

N/A

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 Number: 09-206 Facility, space, and equipment inspection, maintenance, and service records.
Records documenting inspection, maintenance, service, and repair activities relating to buildings, grounds, Federally owned and operated housing, equipment, and personal property.
Disposition: Destroy when 3 years old, but longer retention is authorized if required for business use.
Disposition Authority: DAA-GRS-2016-0011-0008

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 I 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.