US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

08/26/2025

OPDIV:

NIH

Name:

NIAID Vaccine Pilot Plant Support Systems (VPPSS)

PIA Unique Identifier:

P-8606061-231624

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?

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 National Institute of Allergy and Infectious Diseases (NIAID) The NIAID Vaccine Pilot Plant (VPP) Support Systems (VPPSS) boundary consists of the NIAID Freezer Inventory Management System (NFIMS), which is a minor child application system supported by the Commercial-off-the-Shelf (COTS) application FreezerWorks. This application maintains the databases that store all summary data as well as the inventory of clinical trial samples. This information is a key component of the Vaccine Immunology Program (VIP)'s Division of the Vaccine Research Center (VRC) in that the application manages the clinical sample workflow to ensure proper chain of custody from the reception stage to results reporting completion. FreezerWorks also provides an inventory which allows traceable storage and retrieval capability.

The NIAID VPP Support Systems' boundary is housed on-prem within a virtual machine that is hosted by the NIAID Office of Cyber Infrastructure and Computational Biology (OCICB) in the NIAID Research and Development Computing Facility (RDCF). The Office of Engineering Branch (OEB)'s AppHosting team is responsible for the current operation and management of the virtual machine.

The NIAID VPP Support Systems' boundary was formerly a part of the Bioinformatics and Computational Biosciences (BCBB) VIP Laboratory Information Management System (LIMS) system boundary prior to July 2024, at which time the system segmented into its own boundary by the NIAID Cyber Security Program (CSP). The FreezerWorks application was renamed in September 2024 to the NIAID Freezer Inventory Management System (NFIMS) and is now maintained by the Clinical Informatics Branch (CIB).

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

The NIAID Vaccine Pilot Plant (VPP) Support Systems (VPPSS) boundary consists of the NIAID Freezer Inventory Management System (NFIMS), which is a minor child application system supported by the Commercial-off-the-Shelf (COTS) application FreezerWorks. This application maintains the databases that store all summary data as well as the inventory of clinical trial samples. This information is a key component of the Vaccine Immunology Program (VIP)'s Division of the Vaccine Research Center (VRC) in that the application manages the clinical sample workflow to ensure proper chain of custody from the reception stage to results reporting completion. FreezerWorks also provides an inventory which allows traceable storage and retrieval capability.

The personally identifiable information (PII) maintained in the system includes user's first and last name, email address, and username, which are necessary to conduct investigations and track user activity.

Users log in to the NFIMS application 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 National Institute of Allergy and Infectious Diseases (NIAID) The NIAID Vaccine Pilot Plant (VPP) Support Systems (VPPSS) boundary consists of the NIAID Freezer Inventory Management System (NFIMS), which is a minor child application system supported by the Commercial-off-the-Shelf (COTS) application FreezerWorks. This application maintains the databases that store all summary data as well as the inventory of clinical trial samples. This information is a key component of the Vaccine Immunology Program (VIP)'s Division of the Vaccine Research Center (VRC) in that the application manages the clinical sample workflow to ensure proper chain of custody from the reception stage to results reporting completion. FreezerWorks also provides an inventory which allows traceable storage and retrieval capability.

The NIAID VPP Support Systems' boundary is housed on-prem within a virtual machine that is hosted by the NIAID Office of Cyber Infrastructure and Computational Biology (OCICB) in the NIAID Research and Development Computing Facility (RDCF). The Office of Engineering Branch (OEB)'s AppHosting team is responsible for the current operation and management of the virtual machine.

The NIAID VPP Support Systems' boundary was formerly a part of the Bioinformatics and Computational Biosciences (BCBB) VIP Laboratory Information Management System (LIMS) system boundary prior to July 2024, at which time the system segmented into its own boundary by the NIAID Cyber Security Program (CSP). The FreezerWorks application was renamed in September 2024 to the NIAID Freezer Inventory Management System (NFIMS) and is now maintained by the Clinical

Informatics Branch (CIB).

The PII maintained in the system includes user's first and last name, email address, and username, which are necessary to conduct investigations and track user activity.

Users log in to the NFIMS application 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
Username

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?

<100

For what primary purpose is the PII used?

The PII in the system is limited to the user's first and last name, email address, and username, which are necessary to conduct investigations and track user activity.

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

Not applicable (N/A)

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

42 U.S.C. 241

Are records on the system retrieved by one or more PII data elements?

No

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
In-Person
Government Sources
Within the OPDIV

Identify the OMB information collection approval number and expiration date

N/A

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.

NFIMS is not the source system. The NIH Enterprise Directory and IAM are the source systems. Each maintain their own PIAs. Individuals are notified that their PII will be collected when they enter into a business relationship with NIH.

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.

Those individuals who do not wish to have their PII utilized understand that they will not be provided an NFIMS application user account.

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

Business Owners and System Owners are the owners of the data within and they are responsible for all communications that would notify the users of any changes to the system and the data therein.

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.

The NFIMS application is configured to limit PII only to the user's first and last name, email address, and username and does not share any of this information. If a user wants to change their PII, the user would have to contact NIH to change their PII within the OPDIV. Once the record is changed, the System Administrators can update the user's account to reflect the changes.

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 NFIMS application is configured to limit PII only to the user's first and last name, email address, and username and does not share any of this information. The annual review of all user accounts within the NFIMS application is completed at the end of each calendar year and during that review, the data is confirmed for accuracy and availability is limited to those who require access.

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 to PII information on the system is role based, with minimum required access assigned. Access is provisioned as requested in the access request email, which is submitted by leadership.

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 information on the system is role based, with minimum required access assigned. If the user does not have the roles needed to access parts of the system where PII is located, the system will not show them that it exists.

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).

Role based training for administrators of the system as defined by the NIH Information Security Program.

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 number 07-204: System access records. 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. Includes records such as user profiles, log-in files, password files, audit trail files and extracts, system usage files, and cost-back files used to assess charges for system use. Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use. Disposition Authority: DAA-GRS-2013-0006-0004

Process to dispose of this information would only occur in the event that the VPPSS boundary was to be decommissioned, at which point, CIB and the Office of Engineering (OEB) would utilize the NIAID Decommissioning Processes to complete those activities.

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

Administrative: Documented processes have been in place to determine and grant the appropriate role-based access to all data, including PII housed within the system. This access will be reviewed periodically as defined in process documentation to validate the continued access to the system and the PII.

Technical: Users who have the appropriate role/group permissions have the ability to view PII data, while those that do not have such access cannot view PII. All data is contained to the NFIMS application.

Physical: The system is housed on-prem within a virtual machine that is hosted by NIAID Office of Cyber Infrastructure and Computational Biology (OCICB) in the NIAID Research and Development Computing Facility (RDCF). Only members of OEB are permitted to access the on-prem virtual machine.