US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

02/19/2026

OPDIV:

NIH

Name:

NIH Business Intelligence System

PIA Unique Identifier:

P-7096551-160675

The subject of this PIA is which of the following?

Major Application

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

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

The Privacy Impact Assessment is being submitted for review to update the security authorization date.

It is also being updated to reflect the use of Qlik Sense for data analytics for the system.

Describe the purpose of the system.

The National Institutes of Health (NIH) Business Intelligence System (NBIS) is an enterprise-wide administrative business intelligence and analytics solution to multiple stakeholders across the National Institutes of Health (NIH) community including executives, management, and operational staff to meet their specific data and reporting needs. The NBIS functions as a centralized data distribution hub and data broker, providing integrated data on a unified platform that facilitates the daily administration and scientific operations of the NIH Community. NBIS pulls data from multiple NIH source systems into one consolidated, secured, and accessible location. This information drives

advanced analytics and ad-hoc capabilities, allowing for interactive dashboard and customized NBIS web applications: nSIGHT Human Resources (HR) and nSIGHT Finance, which empowers the NIH to make informed business decisions and maximize efficiencies.

Source systems consist of the following federal information systems: National Institutes of Health Business System (NBS), NIH Visiting Scientists Tracking Automation System (nVistas), Accounting for Pay System (AFPS), Electronic Research Administration (eRA), NIH Enterprise Directory (NED), and Office of Human Resources (OHR) systems. Each source system maintains its own unique PIA and NBIS only imports information from the source systems.

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

The agency collects both administrative and financial data. This data is collected from NIH source systems (NBS, nVista, AFPS, eRA, NED, and OHR systems) and includes Social Security Number (SSN), name, email, phone number, education records, military status, taxpayer Identifier (ID), Date of Birth (DoB), photographic IDs, mailing address, financial account information, device IDs, employment status; and is used for business reporting purposes. This data is used for support, reporting and auditing purposes throughout NIH and NIH's Institutes and Centers (IC). Each source system maintains its own unique PIA and NBIS only imports information from the source systems.

NBIS uses Qlik Sense for data analytics, allowing NIH users the ability to combine and load data for fast-track reporting analysis. Qlik Sense transforms data into visually appealing, interactive visualizations and dashboards. Qlik Sense maintains its own Privacy Impact Assessments.

Users log into NBIS 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 the NIH 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 NIH 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 Institutes of Health (NIH) Business Intelligence System (NBIS) is an enterprise-wide administrative business intelligence and analytics solution to multiple stakeholders across the National Institutes of Health (NIH) community including executives, management, and operational staff to meet their specific data and reporting needs. The NBIS functions as a centralized data distribution hub and data broker, providing integrated data on a unified platform that facilitates the daily administration and scientific operations of the NIH Community. NBIS pulls data from multiple NIH source systems into one consolidated, secured, and accessible location. This information drives advanced analytics and ad-hoc capabilities, allowing for interactive dashboard and customized NBIS web applications: nSIGHT Human Resources (HR) and nSIGHT Finance, which empowers the NIH to make informed business decisions and maximize efficiencies.

The agency collects both administrative and financial data. This data is collected from NIH source systems (NBS, nVista, AFPS, eRA, NED, and OHR systems) and includes Social Security Number (SSN), name, email, phone number, education records, military status, taxpayer Identifier (ID), Date of Birth (DoB), photographic IDs, mailing address, financial account information, device IDs, employment status; and is used for business reporting purposes. This data is used for support, reporting and auditing purposes throughout NIH and NIH's Institutes and Centers (IC). Each source system maintains its own unique PIA and NBIS only imports information from the source systems.

NBIS uses Qlik Sense for data analytics, allowing NIH users the ability to combine and load data for

fast-track reporting analysis. Qlik Sense transforms data into visually appealing, interactive visualizations and dashboards. Qlik Sense maintains its own Privacy Impact Assessments.

Users log into NBIS 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 NIH 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 NIH 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
E-Mail Address
Mailing Address
Phone Numbers
Financial Accounts Info
Education Records
Device Identifiers
Military Status
Employment Status
Taxpayer ID

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?

100,000-999,999

For what primary purpose is the PII used?

To verify the user's identity, and enable NIH personnel to perform data operations and business analytics.

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

No Secondary Uses

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

5 U.S.C. 1302, 2951, 4118, 4308, 4506, 7501, 7511, 7521 and Executive Order 10561; Budget and Accounting Act of 1950 (Pub. L. 81-784); Debt Collection Act of 1982 (Pub. L. 97-365); Debt Collection Improvement Act of 1996 (Pub. L. 104-134, sec. 31001). 44 U.S.C 3101 & 3102.

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.

09-90-1402, HHS Payroll Records, HHS/OS,

09-90-0024: Financial Transactions of HHS Accounting and Finance Offices

OPM/GOVT-1: General Personnel Records

Identify the sources of PII in the system.

Government Sources

Within OpDiv

Identify the OMB information collection approval number and expiration date

Not applicable. An OMB collection approval number is not needed as NBIS only uses the PII of Federal employees and direct contractors for internal use only.

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.

Memorandums of Understanding (MOUs) have been obtained from the National Institutes of Health Business System (NBS), NIH Visiting Scientists Tracking Automation System (nVistas), Accounting for Pay System (AFPS), Electronic Research Administration (eRA), NIH Enterprise Directory (NED), and the Office of Human Resources (OHR) systems, to provide the data needed to support the mission of NIH.

If following conditions are met, then there is no need for MOU:

Both the systems should be within the same Boundary, the connection established between both the systems should reside within the same boundary and system boundary controls should be the same for the established connection and the systems and both systems should have the same security controls at the perimeter.

System Categorization of both the systems should be the same.

There should not be flow of sensitive data between the systems.

Both systems should have the security agents as per the NIH policy.

Describe the procedures for accounting for disclosures.

NBIS and source system's teams (NBS, nVista, AFPS, eRA, NED, and OHR systems) are in constant communication regarding the data and changes in that data or access permissions granted to users. For each user log-in there are specific access limitations based on the user role that NBIS and the source systems have designated for the user. Additionally, NBIS maintains audit trail logs for information shared with source systems.

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

Users sign the NBIS registration form, consenting to the use of PII for NBIS registration purposes. When a major change occurs to the NBIS system, users are notified by email. A privacy statement is posted on the NBIS website.

Each individual whose information is stored in NBIS and source systems has given personal

information upon hiring. Notice of information collection is given at the time of acceptance of employment at the NIH.

Information that is pulled from the NIH Enterprise Directory (NED) is voluntarily submitted and entered by an Administrative Officer or by the employee.

All source systems maintain their own approved PIAs on record, including all legal authorities documented.

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.

NBIS is provided PII as part of the data feeds from the source systems (NBS, nVista, AFPS, eRA, NED, and OHR systems) that collect PII from individuals. All of the source systems are responsible for providing methods for individuals to opt-out of the collection or use of their PII.

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

Individuals are notified about how their PII is used via the privacy notice which explains in detail what information is stored and how it is used within NBIS.

Current system users/administrators are given notice via e-mail when major system changes occur.

Information that is pulled from NED is available to be changed by the individual or an individual can reach out to their Administrative Officer to update their NED profile.

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.

A customer support system is in place either phone or e-mail to contact the NIH Information Technology (IT) Service Desk to register inaccuracies, complaints, or issues. Additionally, two staff members assigned to NBIS provide specific NBIS customer service support.

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

Maintaining up to date agreements with the NBIS source systems (NBS, nVista, AFPS, eRA, NED, and OHR systems) to ensure changes in the source system are accurately reflected in the NBIS. Also, periodic user focus group meetings are held to validate business rules and need for the PII, as well as adjust when needed.

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.

System Administrator users are approved by Business Application Services (BAS) management for access based on their technical/functional role in administering, developing, and supporting business

analytics pertaining to PII data.

Institutes and Center (IC) end-users request specific access to NBIS, and their IC Executive Officer or proxy determines and authorizes who may access the proprietary data and what level of access.

NIH Login is required. Following login, system user's privileges are verified through the use of the IAM. IAM has its own approved PIA on record, including all legal authorities documented.

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.

Periodic review of system users' roles to assure access is current with their technical/functional role in administering, developing, and supporting business analytics pertaining to PII data. Additionally, each Institutes and Center (IC) Executive Officer or proxy determines who may access the proprietary data and what level of access.

NIH Login is required. Following login, system user's privileges are verified through the use of the IAM. IAM has its own approved PIA on record, including all legal authorities documented.

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 and Administrator security 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).

Users are offered additional functional training through the NBIS specific business areas within NBIS. Additionally, NBIS offers online tutorials, job aids, and student guides.

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 maintained within NBIS for a time of no less than six years after the project, activity, or transaction is completed or superseded, but longer if retention is authorized for needed business uses in accordance with NARA record retention schedule: 08-102, Records management program records: DAA-GRS-2013-0002-0007

Records are maintained within NBIS for a time of no less than three years after records related to managing financial activities and reports in accordance with NARA record retention schedule: 05-101, Financial management and reporting administrative records: DAA-GRS-2016-0013-0001

Records are maintained within NBIS until business use ceases in accordance with NARA record retention schedule:
07-203, System access records; Systems not requiring special accountability for access: DAA-GRS-2013-0006-0003

Records are maintained within NBIS for a time of no less than six years after a password is altered or an user account is terminated in accordance with NARA record retention schedule: 07-204, System access records; Systems requiring special accountability for access; DAA-GRS-2013-0006-0004

Records are maintained within NBIS for one year after the system is superseded by a new iteration or when no longer needed for agency/Information Technology (IT) administrative purposes to ensure

a continuity of security controls throughout the life of the system in accordance with NARA record retention schedule: 07-201, Systems and data security records: 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 include Security Assessment and Authorization, a System Security Plan, a Contingency Plan, system backups, and documented procedures.

Technical controls include a User Identity Document (ID) and strong password to access the system, and access is only granted when there is a documented approval by an authorized official. Other technical controls include Encrypted data, Firewalls, and Virtual Private Network (VPN).

Physical controls to the server room include guards, ID Badges, Key Cards, and locks.