US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

07/29/2025

OPDIV:

NIH

Name:

NIH Business System Cloud

PIA Unique Identifier:

P-8980142-622688

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 PIA is being updated to reflect a additional System of Records Notice.

Describe the purpose of the system.

The purpose of the NIH Business System (NBS) is to facilitate and support the scientific and research mission of the National Institutes of Health (NIH), an Operating Division of the U.S. Department of Health and Human Services (HHS). NBS is the central electronic business system of the NIH including the general ledger, finance, budget, procurement, supply, travel, and property management systems. NBS delivers centralized administrative support that is cost effective, accurate and timely. NBS provides qualitative and quantitative benefit to the NIH with the purpose of refining and improving business processes. NBS scope includes the following business or functional areas:

Financial Management; Property Management; Accounts Payable (Commercial Accounts);

Acquisitions; Service and Supply Funds Operations; Supply Management; and Travel Management.

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

NBS collects, maintains, and shares information required for functionality and business purposes including name, Social Security number (SSN) or employer identification number/taxpayer identification number (EIN/TIN), address, email address, phone number, purpose of payment or request for payment, bank account and routing numbers, accounting classification and the amount paid or billed. Information is also collected in the event of an overpayment and for outstanding charges, fees, loans, grants, or scholarships, the amount of the indebtedness, the repayment status and the amount to be collected. In the event of an administrative wage garnishment, information about the debtor's employment status and disposable pay available for withholding will be maintained.

NBS pulls the following information from the NIH Enterprise Directory (NED) which maintains its own unique Privacy Impact Assessment (PIA): first name, last name, middle name, NED ID, SSN, date of birth, employee type, (i.e., volunteer, Fellow, Contractor, or Federal employee), EIN, email address, home address, work address, and phone number.

Banking information for employees is received via the Automated Clearing House (ACH) interface. Which includes the SSN, name, bank account number, routing number.

Users log in to this system using the NIH Identity, Credential, and Access Management (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. Additionally, NBS pulls the following data elements from NIH IAM: name, employment status, and EIN.

NBS also collects application specific login credentials including a username and password.

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

The purpose of NBS is to facilitate and support the scientific and research mission of the NIH, an Operating Division of the U.S. HHS. NBS is the central electronic business system of the NIH including the general ledger, finance, budget, procurement, supply, travel, and property management systems. NBS delivers centralized administrative support that is cost effective, accurate and timely. NBS provides qualitative and quantitative benefit to the NIH with the purpose of refining and improving business processes. NBS scope includes the following business or functional areas:

Financial Management; Property Management; Accounts Payable (Commercial Accounts); Acquisitions; Service and Supply Funds Operations; Supply Management; and Travel Management.

NBS collects, maintains, and shares information required for functionality and business purposes including name, SSN or EIN/TIN, address, email address, phone number, purpose of payment or request for payment, bank account and routing numbers, accounting classification and the amount paid or billed. Information is also collected in the event of an overpayment and for outstanding charges, fees, loans, grants, or scholarships, the amount of the indebtedness, the repayment status and the amount to be collected. In the event of an administrative wage garnishment, information about the debtor's employment status and disposable pay available for withholding will be maintained.

NBS pulls the following information from the NED which maintains its own unique PIA: first name, last name, middle name, NED ID, SSN, date of birth, employee type, (i.e., volunteer, fellow, contractor, or Federal employee), EIN, email address, home address, work address, and phone number.

Banking information for employees is received via the ACH interface. Which includes the SSN, name, bank account number, routing number.

Users log in to this 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. Additionally, NBS pulls the following data elements from NIH IAM: name, employment status, and EIN.

NBS also collects application specific login credentials including a username and password.

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
Name
E-Mail Address
Phone Numbers
Financial Accounts Info
Employment Status
Taxpayer ID
User credentials; Employee ID
Personally identifiable information (PII) collected is stored for financial reporting and payments. PII is not solicited directly and is pulled from NIH NED and NIH IAM.

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
No

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

The primary purpose of collecting, sharing, and maintaining personally identifiable information (PII) in NBS is to support the functions inherent in an enterprise financial system. The records are used to keep track of all payments to individuals, exclusive of salaries and wages.

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

Records are also used internally to develop reports for the Internal Revenue Service (IRS) and applicable State and local taxing officials of taxable income.

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

42 U.S.C. §§ 241, 248, 282 and 284

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.

09-90-0024, HHS Financial Management System Records

09-25-0217 NIH Business System (NBS)

Identify the sources of PII in the system.

Government Sources
- Within OpDiv
- Other Federal Entities
- Other Federal Sources
- Public
- Private Sector

Identify the OMB information collection approval number and expiration date

Not applicable

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.

NBS has several agreements in place that authorize specific information sharing and/or disclosure, as follows:

Citibank

General Services Administration (GSA):
Concur Government Edition (CGE)
Federal Procurement Data System (FPDS)
System for Award Management (SAM)

Department of Treasury:
Government (G) Invoicing
Invoice Processing Platform (IPP)
Payment Automation Management (PAM)

HHS:
Accounting for Pay System (AFPS)
BuySmarter
Learning Management System (LMS)
Payment Management System (PMS)
Financial Business Intelligence System (FBIS)

NIH:
Learning Management System (LMS)
Loan Repayment Programs (LRP)
NIH Enterprise Directory (NED)
Administrative Management Budget Information System (AMBIS)
electronic Research Administration (eRA)
nVision
Center for Information Technology (CIT)
Royalties Management System (ROMANSYS)
Research Volunteers Payment System (RVPS)
Secure Payment Registration System (SPRS)
Scientific Research Evaluation (SREA)
Self Service Store (SSS)
Division of Veterinary Resources Billing System (DVRBS)
Purchasing Online Tracking System (POTS)

Describe the procedures for accounting for disclosures.

The NBS System Owner maintains audit logs which track all requests for disclosures of PII.

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

All persons who enter in business relationships with NIH are informed in writing prior to the beginning of the transaction that PII is required in order to proceed.

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.

Due to the essential operations of the NBS, individuals who enter a business relationship with NIH do not have an option to object to the collection of their PII.

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

The NBS Administrative Officer has the responsibility for records maintenance and the role of initiating contact using the NIH Secure Email File Transfer (SEFT) Service.

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 NIH IT Service Desk if they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.

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

As part of the NIH required Annual Assessment process, NBS conducts periodic reviews by the system owner, the system information system security officer (ISSO) and the NIH privacy officer to review the PII contained in the system. This review ensures each of the following elements are addressed; integrity, availability, accuracy and relevancy.

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.

Specific procedures in place to limit access of PII are based on the following:

Role-based access control mechanisms.
Separation of duties analysis.
User provisioning protocols.
System administrator access is limited to functional subject matter experts (SMEs).
Developers/direct contractors have planner access in the user interface and have access to all data coming through interfaces from the travel system to the financial system.
Access is limited to those responsible for maintaining the interfaces.
Other direct contractors have access to the financial data that is in the financial system - this is limited by the role of the direct contractor.

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.

NBS utilizes role-based access control to control access to PII. NBS increased security protections by implementing additional data masking for PII in the system in 2022.

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. There are five categories of mandatory information technology (IT) training (Information Security, Counterintelligence, Privacy Awareness, Records Management and Emergency Preparedness. 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).

Periodic training updates are provided to active users when application enhancements are implemented throughout the year and annually with application version upgrades. All NIH users are exposed to records, security, and privacy awareness through ongoing phishing exercises.

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 following Finance and Budget General Record Schedule (GRS) record retention schedules:

Item 05-102: Financial Transaction Records Related to Procuring Goods and Services, Paying Bills, Collecting Debts, and Accounting. Official Record Held in the Office of Record. Destroy 6 years after

close of fiscal year, but longer retention is authorized if required for business use.
DAA-GRS-2013-0003-0001

Item 05-104: Financial transaction records related to procuring goods and services, paying bills, collecting debts, and accounting. All other copies. Destroy when business use ceases.
DAA-GRS-2013-0003-0002

Item 05-106: Records supporting compilation of agency financial statements and related audit, and all records of all other reports. Destroy 2 years after completion of audit or closure of financial statement/ accounting treatment/issue, but longer retention is authorized if required for business use.
DAA-GRS-2013-0003-0011

Item 05-107: Property, plant and equipment (PPE) and other asset accounting. Destroy 2 years after asset is disposed of and/or removed from agency's financial statement, but longer retention is authorized if required for business use.
DAA-GRS-2013-0003-0004

Item 05-108: Cost accounting for stores, inventory, and materials.
Destroy when 3 years old, but longer retention is authorized if required for business use.
DAA-GRS-2013-0003-0012

Item 05-203: Budget execution records. Records created and held by offices that prepare an agency' s budget proposal for the White House. Destroy 6 years after close of fiscal year, but longer retention is authorized if required for business use.
DAA-GRS-2015-0006-0002

Item 05-208: Budget administration records. Records any office creates and holds. Destroy when 3 years old, but longer retention is authorized if required for business use.
DAA-GRS-2015-0006-0007

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. All privileged accounts are certified biennially by NBS management and system owner. All users must sign and adhere to the NIH Rules Of Behavior. Access to any NBS system or applications must be authorized by NBS Federal Management or Federal leads and are continuously monitored and reported weekly.

Physical Controls:
The information technology (IT) hardware used to host NBS protected information is located in a secured NIH datacenter facility. The facility is open to authorized personnel only whose access is monitored by locked doors with badge readers for both ingress and egress. Each ingress and egress event is logged for after the fact investigations. Additionally, the NIH hosting facility is under 24-hour surveillance for physical security and environmental hazards.

Technical Controls:
IT hardware and software is segmented from public networks to prevent unauthorized or malicious access from outside NIH. NIH implements a variety of network, hardware and software applications

for intrusion detection and prevention, to include virus malware protections, and data loss prevention. NBS monitors access controls lists and event logs to detect unauthorized, suspicious or malicious activity on a daily basis. Access lists are restricted to approved IT technical personnel only. Personal Identity Verification (PIV) authentication must be used for access and only through NIH Virtual Private Network (VPN) services. Data at rest is protected through Oracle Transparent Data Encryption (TDE) and data in transit by Transport Layer Security (TLS) 1.3, which is Federal Information Processing Standard (FIPS) 140-2 compliant or Secure File Transfer Protocol (SFTP) 256AES encryption or NIH Center for Information Technology (CIT) Webservices, all FIPS 140-2 compliant. To further secure users Data, NBS has implemented data redaction for PII.