US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

06/30/2025

OPDIV:

NIH

Name:

Background Investigation Tracking System

PIA Unique Identifier:

P-5455206-847474

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.

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

Significant System Management Change

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

The Background Investigation Tracking System (BITS) has a new point of contact (POC). The parent boundary was changed from Security and Emergency Response General Support System (SER GSS) to ORS/ORF Applications Environment-Moderate (OAEM). BITS' functions remain unchanged.

Describe the purpose of the system.

The purpose of the Background Investigation Tracking System (BITS) is to systematically track personnel security and access control actions associated with individual's requests for physical and logical access to National Institutes of Health (NIH). The required database tracks individuals who have either completed, or are currently involved in the personnel security process. The personnel security process includes two types of investigations: to provide a basis for agencies to determine

whether a person should be granted a security clearance, and to provide a basis for determining a person`s suitability for Federal employment. Additionally, BITS is used to track life-cycle activities of the Personal Identity Verification (PIV) credentials as well as the scheduling for background investigation and PIV related activities.

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

BITS collects Social Security Number (SSN), Name, Driver License Number, Mother Maiden Name, E-Mail Address, Phone Numbers, Medical Notes, Education Records, Military Status, Foreign Activities, Date of Birth, Mailing Address, Medical Records Number, Financial Account Info, Legal Documents, Employment Status, Passport Number, photo identification, and finger prints.

BITS only shares transactional data with the NIH Enterprise Directory (NED). The transaction data consists of items such as a record flag to indicate that a applicant is ready for badge issuance or dates when the fingerprint check are completed. No documentation related to the applicant's background investigation is shared. NED maintains it's own privacy impact assessment

Users Log into the system 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 a encrypted format. The IAM Services are a 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 purpose of the Background Investigation Tracking System (BITS) is to systematically track personnel security and access control actions associated with individuals requests for physical and logical access to National Institutes of Health (NIH). The required database tracks individuals who have either completed, or are currently involved in the personnel security process. The personnel security process includes two types of investigations: to provide a basis for agencies to determine whether a person should be granted a security clearance, and to provide a basis for determining a person`s suitability for Federal employment. Additionally, BITS is used to track life-cycle activities of the Personal Identity Verification (PIV) credentials as well as the scheduling for background investigation and PIV related activities.

BITS collects Social Security Number (SSN), Name, Driver License Number, Mother Maiden Name, E-Mail Address, Phone Numbers, Medical Notes, Education Records, Military Status, Foreign Activities, Date of Birth, Mailing Address, Medical Records Number, Financial Account Info, Legal Documents, Employment Status, Passport Number, photo identification, and finger prints.

BITS only shares transactional data with the NIH Enterprise Directory (NED). The transaction data consists of items such as a record flag to indicate that a applicant is ready for badge issuance or a dates when the fingerprint check are completed. No documentation related to the applicant's background investigation is shared.

Users Log into the system 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 a encrypted format. The IAM Services are a 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.

Social Security Number
Date of Birth
Name
Photographic Identifiers
Driver's License Number
Mother's Maiden Name
E-Mail Address
Mailing Address
Phone Numbers
Medical Records Number
Medical Notes
Financial Accounts Info
Legal Documents
Education Records
Military Status
Employment Status
Foreign Activities
Passport Number
finger prints

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

Employees
Public Citizens
Vendor/Suppliers/Contractors
Fellows, Guest Researchers, Volunteers

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

The BITS system uses Personally identifiable information (PII) to systematically track personnel security and access control actions associated with individuals requesting access to NIH as part of the background investigation process.

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

The secondary use of the PII is for PIV card inventory tracking.

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

5 U.S.C. 3301, 3302, 7301; Executive Order 10577; Executive Order 11222; Executive Order 12968

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.

GSA/GOVT-7, Personal Identity Management Systems.

OPM/GOVT-9, File on Position Classification Appeals, Job Grading Appeals, Retained Grade or Pay

09-90-0020, Suitability for Employment Records, HHS/OS/ASPER

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Online

Government Sources

Within the OPDIV

Other Federal Entities

Non-Governmental Sources

Public

Identify the OMB information collection approval number and expiration date

1615-0047, Employment Eligibility Verification: 05/31/2027

3206-0182, Declaration for Federal Employment: 08/31/2026

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.

The Memorandum of Understanding (MOU) - Background Investigation System (BITS) and the NIH Enterprise Directory (NED). Data traverses a secure connection containing identity, organization, contact and locator information as well as privacy act data.

The Memorandum of Understanding (MOU) - Defense Counterintelligence Security Agency (DCSA) and the Division of Personnel Security and Access Control (DPSAC). Completed DCSA background investigation files are transmitted unidirectionally through an encrypted tunnel establishing a system-to-system connection with DPSAC.

The Memorandum of Understanding (MOU) - NIH Center for Information Technology (CIT) Identity and Access Management (IAM) Identity Management Service (IMS) Virtual Directory Service (VDS) and NIH ORS Background Investigation Tracking System (BITS). The interconnection between CIT IAM and the OD ORS is to establish a bridge between the NIH IAM IMS VDS and the ORS ITB BITS Database. The driver for this requirement is the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) program to manage trust in people granted access (TRUST). The TRUST security capability reduces the risk of a loss in data availability, integrity, and confidentiality. It ensures only properly vetted users are given access to systems and credentials. Specifically, in support of the CDM initiative, NIH must consolidate a person's security related behavior information in a master user record (MUR).

Describe the procedures for accounting for disclosures.

BITS, OPM, and NED conducts periodic internal and external audits of the IT systems to

identify and mitigate vulnerabilities. Production application systems and data are protected by a robust disaster recovery plans. A test of this plan is conducted annually to ensure its effectiveness, test new capabilities, reveal weaknesses, keep Information Technology (IT) staff and customers familiar with disaster recovery procedures, and to verify that all disclosures were authorized.

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

Submission of the personal information is voluntary. However, the absence of required information may impact ability for the individual to be hired or be identity proofed for their badge issuance.

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.

The information collected is obtained from the actual individuals. Information is not obtained through observation.

The collection and use of information gathered from system interfaces, and manually entered by BITS staff is required as part of the job application and background investigation processes. Notice of information collection is given at the time of applying for, and acceptance of, employment at the NIH.

PII are collected shared only with officially designated HSPD-12 Sponsors, Adjudicators and Issuers.

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

The collection and use of information gathered from system interfaces, and manually entered by BITS staff is required as part of the job application and background investigation processes. Notice of information collection is given at the time of applying for, and acceptance of, employment at the NIH. Individuals can chose to not give their information by not applying for a job position.

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 who is concerned that his/her information may have been inappropriately obtained , used , or disclosed, or that the information is inaccurate may write, email or appear in person to see the Director of the Personnel Security Branch. The inquiry must contain name and a copy of an I-9 identifying document along with the reason for concern. The issue will be investigated and the results of the investigation will be provided in writing to the concerned individual.

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

Periodic audits are conducted to ensure the BITS' data's 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.

System users are approved for access and permissions based on their functional role in BITS using the principle of least privilege.

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.

End user access to PII is granted based on role and function in the workflows, and is granted at the lowest level needed to perform a user's designated role in the workflow.

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).

Each module has a data owner who is assigned the responsibility for ensuring training is conducted. This training includes: user guides, Standard Operating Procedures (SOPs), and continuous situation specific user training.

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: 09-422, Personnel security investigative reports. Personnel suitability and eligibility investigative reports. Destroy in accordance with the investigating agency instruction (DAA-GRS-2017-0006-0022).

Item Number: 09-42, Personnel security and access clearance records. Records of people not issued clearances. Destroy 1 year after consideration of the candidate ends, but longer retention is authorized if required for business use (DAA-GRS-2021-0001-0007).

Item Number: 09-425, Personnel security and access clearance records. Records of people issued clearances. Destroy 5 years after employee or contractor relationship ends, but longer retention is authorized if required for business use (DAA-GRS-2021-0001-0008).

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

Administrative Controls: Access requests are managed, validated, and audited by system administrators and scheduled audits are performed to ensure accounts are validated and/or revoked if needed. Access Disclosure Agreements are required for all users.

Technical Controls: Access to the system is controlled by NIH log-in which authenticates the user prior to granting access. Access level and permissions are controlled by the system and based on user, role, organizational unit, and status of the report. All servers have been configured to remove all unused applications and system files and all local account access except when necessary to manage the system and maintain integrity of data.

Physical Controls: The servers reside in the Center for Information Technology (CIT) Computer Room where policies and procedures are in place to restrict access to the machines. This includes guards at the front door and entrance to the machine room.