US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/07/2025

OPDIV:

NIH

Name:

Integrated Time and Attendance System

PIA Unique Identifier:

P-4600558-166559

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.

Based on the business and technical support team's understanding, the Integrated Time and Attendance System (ITAS) has had no major changes since the last submission in 2018.

Describe the purpose of the system.

The Integrated Time and Attendance System (ITAS) is an automated federal timekeeping system at the National Institutes of Health (NIH). Users have access to real-time leave balances and it ensures accurate recording of work activity by enforcing time and attendance policies and procedures specific to the Federal Government. ITAS interconnects with the NIH Enterprise Directory (NED) through NIH’s business intelligence and analytics application nVision. ITAS also makes a biweekly timecard submission to the Department of Health and Human Services (HHS) Payroll Interface. The HHS Payroll system, in turn, relays select data downstream to the Defense Finance and Accounting Service (DFAS) payroll system.

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

ITAS collects employee names, Social Security Numbers (SSN), hours worked, leave hours earned and used, sick leave hours earned and used, agency code, Standard Administrative Code, Leave Approving Official's name, Timekeeper's name, work email address, organization, employment status, and medical condition information if authorized through the Voluntary Leave Transfer Program (VLTP) process. All employee information is manually transferred into ITAS by the Timekeeper or Administrative Officer (AO) from a source system: NED, which is collected during the on-boarding process, or the VLTP. Personally Identifiable Information (PII) is used for leave tracking and submission of it is required to permit payroll processing for employees. All source systems maintain their own and unique Privacy Impact Assessment (PIA), including all legal authorities documented.

Users log in to this 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 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.

ITAS is an automated federal timekeeping system at NIH. Users have access to real-time leave balances and it ensures accurate recording of work activity by enforcing time and attendance policies and procedures specific to the Federal Government. ITAS interconnects with the NIH NED through nVision. ITAS also makes a biweekly timecard submission to HHS Payroll Interface. The HHS Payroll system, in turn, relays select data downstream to DFAS payroll system.

ITAS collects employee names, SSN, hours worked, leave hours earned and used, sick leave hours earned and used, agency code, Standard Administrative Code, Leave Approving Official's name, Timekeeper's name, work email address, organization, employment status, and medical condition information if authorized through the VLTP process. All employee information is manually transferred into ITAS by the Timekeeper or AO from a sources system: NED, which is collected during the on-boarding process, or the VLTP. PII is used for leave tracking and submission of it is required to permit payroll processing for employees. All source systems maintain their own and unique PIA, including all legal authorities documented.

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.

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

Employment Status
Hours worked, leave hours earned and used, sick leave hours earned and used
Agency Code, Standard Administrative Code (SAC), Leave approving Officials name, Time Keepers name, organization, medical condition

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

Employees
Business Partner/Contacts (Federal/state/local agencies)
No

How many individuals' PII is in the system?

50,000-99,999

For what primary purpose is the PII used?

The primary use of the information is to prepare the NIH payroll and compute leave balances. ITAS records are used as the basis for pay and leave actions for the purpose of payroll processing. The payroll cycle is bi-weekly, therefore, every two weeks the ITAS system processes are run to compute and accrue leave earned, generate timecards for the upcoming pay period, and produce an output file to be transmitted to DFAS payroll system via the HHS payroll interface.

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

Not applicable

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

Authority for the maintenance of the system is 5 U.S.C. Chapter 55 and Chapter 63, and 42 U.S.C. 202-217, 218a.

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.

SORN 09-90-1402, HHS Payroll Records

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
Online
Government Sources
Within the OPDIV
Other HHS OPDIV
Other Federal Entities

Identify the OMB information collection approval number and expiration date

An OMB collection approval number is not needed as ITAS only uses the PII of federal employees 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.

Interconnection Security Agreements (ISAs) and/or Memorandums of Understanding (MOUs) exist for all ITAS data interfaces DFAS and NED.

Describe the procedures for accounting for disclosures.

Requests must be submitted in writing to the system manager or NIH Office of Human Resources (OHR). OHR will consult with the NIH Freedom Of Information Act and Privacy Offices as appropriate to assist with determining whether to release any information or records.

Information about such requests will be retained, including the requestors' name and contact information, exactly what information is requested, any information provided in response, and the date of the disclosure. These records will be maintained for the required retention period. Disclosures are unlikely unless they are required to further the primary purpose of the system.

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

Notification and consent occur during the hiring and onboarding process. In addition, the ITAS website contains a notice providing information to users about the system's purpose, authority for collecting information in it, uses of the information, and the effect of any failure to provide necessary information.

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 not a method for individuals to opt-out. PII collected by source systems are required as part of the hiring process and for employment with NIH. Individuals rejecting providing their PII can be denied access.

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

PII is not collected from individual users therefore major changes in ITAS do not require obtaining their consent. No notification procedures are required. If change occurs, notification will be done via the PII source system NED.

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.

PII is imported from the source system NED, which maintains its own processes to resolve issues and can be found in its PIA. NED can be contacted on ned-ops@list.nih.gov

Within the ITAS system, users contact their Timekeeper for assistance with identifying the problem. If the Timekeeper is able to do that, they will generate an error notice to be forwarded to the NIH Benefits and Payroll Liaison Branch to facilitate a resolution.

If the Timekeeper is unable to assist, they will contact the user's Administrative Officer.

If the Administrative Officer is unable to identify the problem, they will contact the ITAS Coordinator for assistance.

If the problem still cannot be resolved, the ITAS Coordinator will contact a Payroll Team member in the Benefits and Payroll Liaison Branch.

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

Bi-weekly data transmission to the Payroll System will identify inconsistent information.

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 is restricted using an authorization process. Only privileged users with administrative rights can access PII. User roles such as Employee, Leave Approving Official, Timekeeper, and ITAS Administrator restrict the functions and screens available to them.

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 are made based on 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.

A NIH IAM Systems account login is required to gain access to the stored PII data.

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).

HHS requires role-based training when responsibilities associated with a given role or position, could, upon exception, have the potential to adversely impact the security posture of one or more HHS systems. HHS has a more rigorous expectation for the training of individuals who develop or manage sensitive systems. These staff receive training based on their specific duties and the technologies they use.

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: 06-403, Time and attendance records.

Description: Sign-in/sign-out records, time cards, leave applications and approvals of all types (annual, sick, family medical, military service, jury duty, leave donations, etc.); overtime, compensatory, and credit time requests and approvals; premium pay authorizations; and other records documenting employees' presence at or absence from work. Disposition Instruction: Destroy when 3 years old, but longer retention is authorized if required for business use.

Disposition Authority: Disposition Authority created by an Agency (DAA)-General Records Schedules (GRS)-2019-0004-0002

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.

Technical controls include the capability to identify users and differentiate among user roles. Based on the least privilege principle, ITAS allows only the accesses and permissions needed to perform specific functions. User roles are linked to Personal Identity Verification (PIV) smartcard authentication. ITAS uses NIH Login and Single Sign-On (SSO), to control authorization and authentication of users. Strict password requirements include expiration after a set period of time, a minimum length, a combination of uppercase, lowercase, and special characters. In addition, accounts are locked after a set number of incorrect attempts.

Physical controls limit access to the servers located in the Center for Information Technology Computer Center. A security guard is stationed at the main entrance of the complex, 24 hours a day, seven days a week. Anyone entering the building must display a valid government identification (ID) showing a current identification photo, or register with the security guard to acquire a temporary visitors badge. All entrance doors to the computer center and the machine rooms are controlled by card-activated locks that restrict access 24 hours a day seven days a week.