US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/10/2026

OPDIV:

NIH

Name:

NIH Enterprise Technology Transfer System

PIA Unique Identifier:

P-7430748-190155

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?

Yes

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 NIH Enterprise Technology Transfer (ETT) system is used to track all aspects of technology transfer conducted at NIH, including invention disclosures, patent prosecutions, invention and patent licensing, technology marketing, procurement, billing, and payments.

NIH ETT consists of the following interfaces: a web application, which is used for most day-to-day work performed in the system, an analytics portal, which is used to generate reports from the database, and a law firm web portal, which allows selected commercial organizations to access Request for Quotation (RFQs) and upload responses.

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

Personally Identifiable Information (PII) and authentication information includes the information necessary to ensure that all persons who are potentially entitled to receive any federal benefit are enumerated and identified so that Federal agencies can have reasonable assurance that they are paying or communicating with the right individuals. For NIH employees, this information includes

name, organization, and NIH Employee Identification number found in the NIH Enterprise Directory (NED) or mailing addresses, as necessary. For members of the public, this information includes name, name of employer, and mailing addresses. Email and phone numbers are collected for all individuals in the system. No financial information regarding individual persons is stored in the system beyond a history of amounts paid to those individuals.

Users log in to ETT 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.

Law Firm users log in using a user ID and password along with an authentication token that is either texted or provided via an authentication app.

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

The NIH Enterprise Technology Transfer (ETT) system is used to track all aspects of technology transfer conducted at NIH, including invention disclosures, patent prosecutions, invention and patent licensing, technology marketing, procurement, billing, and payments.

NIH ETT consists of the following interfaces: a web application, which is used for most day-to-day work performed in the system, an analytics portal, which is used to generate reports from the database, and a law firm web portal, which allows selected commercial organizations to access Request for Quotation (RFQs) and upload responses.

Personally Identifiable Information (PII) and authentication information includes the information necessary to ensure that all persons who are potentially entitled to receive any federal benefit are enumerated and identified so that Federal agencies can have reasonable assurance that they are paying or communicating with the right individuals. For NIH employees, this information includes name, organization, and NIH Employee Identification number found in the NIH Enterprise Directory (NED) or mailing addresses, as necessary. For members of the public, this information includes name, name of employer, and mailing addresses. Email and phone numbers are collected for all individuals in the system. No financial information regarding individual persons is stored in the system beyond a history of amounts paid to those individuals.

Users log in to ETT 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.

Law Firm users log in using a user ID and password along with an authentication token that is either texted or provided via an authentication app.

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
Mailing Address
Phone Numbers
NIH Employee ID number
User IDs and Passwords
Organization

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

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

The information is necessary to ensure that all persons who are potentially entitled to receive any federal benefit are enumerated and identified so that federal agencies can have reasonable assurance that they are paying or communicating with the right individuals.

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

NA

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

Bayh-Dole Act, 37 CFR 401
15 U.S.C. secs. 3710–3710d
35 U.S.C. secs. 200–212

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.

09-90-0067, Invention, Patent, and Licensing Documents Related to Inventions By Public Health

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
In-Person
Hardcopy
Email
Government Sources
Within OpDiv
Other HHS OpDiv
Non-Governmental Sources
Public
Private Sector

Identify the OMB information collection approval number and expiration date

0990-0419 Expiration 10/31/2026

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.

Inventors register their information through the iEdison system that is part of eRA (not an acronym). As part of registration, inventors are required to submit their personal information and informed about the reason for collection and expected uses. eRA maintains its own PIA, including all legal authorities.

Employees of partner organizations submit their contact information in person as part of normal business activity.

Partner employee information is collected as part of contractual negotiations for licensing, materials transfer, and/or research collaborations. It is understood that their information is being stored so that they can be contacted as required for negotiation, execution, and performance under terms of the contract.

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.

eRA is the source for employee information. eRA maintains its own PIA, including processes for opting out of the collection of PII.

For partnered entities, there is no opt-out option. If a company declines to provide a point of contact, they cannot participate in receiving a contract or support.

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

ETT is not the source system for internal employee information eRA is the source system for internal, employee information. eRA maintains its own PIA, including processes to notify and obtain consent when a major change occurs.

The scope of the system will not change. If something does change, it is noted in a modified contract.

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.

ETT is not the source system. eRA is the source system for internal employee information. eRA maintains its own PIA, including processes to resolve concerns of individuals. If an external partner has a concern, they can email the Tech transfer Office at nihott@mail.nih.gov.

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

PII for inventors is validated prior to every distribution of funds. PII for NIH employees is validated against NIH Enterprise Directory (NED). NED maintains its own PIA, including all legal authorities. PII for employees of partner organizations is updated when those individuals provide new 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 granted using security groups. These groups define the type of access (none/read only/edit/create/delete) for different types of records based on the role of the user. Access is further restricted by security collections which limit access to certain specific records to users of specific organizations that own those records.

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.

Privileges are assigned to different roles. Each role is given the lowest level of privilege that will allow users with those roles to perform their routine job functions.

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.

The NIH Security Awareness Training course is used to satisfy this requirement. 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).

Operational role-based training is provided to onboarding personnel by their respective organizations at the Institute, Center, and Office (ICO) level. Customized training videos about how to use the ETT system are available to all system users via the NIH Office of Technology Transfer (OTT) SharePoint site.

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.

04-101. Employee Invention Reports and Patent Applications. Cut off following expiration, lapsing, withdrawal, or abandonment of all issued patents, and patent applications within an associated patent family; or unpatented inventions when not associated with licensable or available licensed research material. Destroy 6 year{s) after cutoff or when no longer needed for business purposes occurs, whichever is later. DAA-0443-2016-0002-0001.

04-102. License Agreement, Cooperative Research and Development Agreement (CRADA) and Other Technology Transfer Agreement Records - Executed Agreements with Financial Terms. Cut off at expiration or termination of the License, CRADA or Technology Transfer Agreement. Destroy 6 year(s) after cutoff or when no longer needed for business purposes occurs, whichever is later. DAA-0443-2016-0002-0002.

04-103. License Agreement, CRADA and Other Technology Transfer Agreement Records - Denied Applications That Are Under Appeal. Cut off at the date of resolution of the appeal. Destroy 7 year(s) after cutoff or when no longer needed for business purposes occurs, whichever is later. DAA-0443-2016-0002-0003.

04-104. License Agreement, CRADA and Other Technology Transfer Agreement Records - Agreements without Financial Terms and Non-executed Agreement Applications. Cut off at: 1) termination of the Agreement or at the expiration of the Agreement term or the Confidentiality term, whichever is longer; or 2) Confirmation that the activities under the Agreement are no longer continuing; or 3) When the Application/ Agreement is withdrawn, the negotiations are terminated, or the license application is denied and there is no appeal. Destroy 3 year(s) after cutoff or when no longer needed for business purposes occurs, whichever is later. DAA-0443-2016-0002-0004.

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

Administrative Controls: Supervisors verify the roles that are assigned to their personnel. ETT Systems Administrators assign the users to security groups based on the assigned roles. Privileges are based on security groups and users can only access the minimum amount of PII necessary to perform their jobs. Standard Operating Procedures governing security groups, permissions, and roles are maintained by the ETT Systems Administration Team.

Technical Controls: Technical Controls: Access to the system is controlled by IAM which authenticates users prior to granting access. Once authenticated, users are given permissions based on the security groups associated with their ETT system user accounts. User activity is monitored and reviewed by ETT Systems Administrators on a weekly basis.

ETT Systems Administrators generate database audit records containing information that establishes the type, time, source, and outcome of an event, and the identity of any individuals or subjects associated with the event. The ETT System maintains and protects audit information and audit tools from unauthorized access, modification, and deletion. Audit logs are protected as sensitive information and retained for an appropriate period of time. ETT Systems Administrators do not have “write” or “delete” access to audit trails.

Physical access: access to all Amazon Web Services data centers and facilities housing IT infrastructure components is restricted to authorized data center employees, vendors, and contractors who require access to perform maintenance activities.

Identify the publicly-available URL:

https://ett.nih.gov
https://lfp.nih.gov

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Does the website have any information or pages directed at children uner the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

No

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

Yes