US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/12/2025

OPDIV:

NIH

Name:

Basic Local Alignment Search Tool (BLAST)

PIA Unique Identifier:

P-9136014-484352

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?

Yes

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.

This validation is intended to refresh content. There have been no substantial changes since the last assessment.

Describe the purpose of the system.

Basic Local Alignment Search Tool (BLAST) is a set of programs designed to perform similarity searches on all publicly available sequence databases.

Researchers regularly use the searches to gain insight into the function and biological importance of gene products. BLAST is able to match a user-submitted unknown sequence against all publicly available sequences and to identify regions of similarity within two sequences.

BLAST is a joint project between the National Library of Medicine (NLM) and the National Center for Biotechnology Information (NCBI).

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

All users access BLAST through Web browser sessions and are limited to read-only access to the sequence databases. Searches are performed in parallel with different databases assigned to different sets of backend servers. The backend servers process the request and identify matches; the results from individual searches are then merged into a single result.. The merged results are stored in the database. After the search is complete, the user returns to BLAST with an assigned token and requests the results. The user-specified format for the results is processed and when complete, is sent back to the search database and returned through the front-end Web servers.

Members of the public can voluntarily submit their name, email addresses and a password to get on the BLAST News List. Giving a name is optional but the user is required to create a password. BLAST news gives short messages announcing updates and new features, along with advance notice about upcoming changes in the BLAST service.

Those requiring specific access to BLAST log in using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (PIA) on record, with 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 collects unique user credentials and stores them in an encrypted format. The IAM Service is 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.

BLAST is a set of programs designed to perform similarity searches on all publicly available sequence databases. Researchers regularly use the searches to gain insight into the function and biological importance of gene products. BLAST is able to match a user-submitted unknown sequence against all publicly available sequences and to identify regions of similarity within two sequences.

All users access BLAST through Web browser sessions and are limited to read-only access to the sequence databases. Searches are performed in parallel with different databases assigned to different sets of backend servers.
Members of the public can voluntarily submit their name, email addresses and a password to get on the BLAST News List. Giving a name is optional but the user is required to create a password. BLAST news gives short messages announcing updates and new features, along with advance notice about upcoming changes in the BLAST service.
Those requiring specific access to BLAST log in using the NIH IAM Services which maintains its own unique PIA on record, with all legal authorities documented.

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
Password

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

Employees
Public Citizens

How many individuals' PII is in the system?

5,000-9,999

For what primary purpose is the PII used?

The primary purpose of the personally identifiable information (PII) is to allow individuals the ability to sign up for emails from BLAST.

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

There is no secondary use of PII.

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

42 U.S.C. section 286, 42 U.S.C. § 282(i) and (j)), 44 U.S.C. Sec. 2904, 42 U.S.C. 241.

Are records on the system retrieved by one or more PII data elements?

No

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
Online
Government Sources
Within the DOC
NCBI BLAST database
Non-Government Sources
Public

Identify the OMB information collection approval number and expiration date

Not applicable. NCBI does not solicit information from the public.

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.

PII is voluntarily submitted by individuals. A confirmation email is sent once an individual subscribes to verify registration.

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.

Individuals may un-subscribe at any time through the website, or through email. Individuals may also reach out to the NCBI Help Desk if they need further assistance.

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

PII within the system is not changed or modified. PII is entered by the individual and may be edited at any time by the individual themselves. Individuals may also reach out to the NCBI Help Desk if they have any questions regarding their information or have concerns that need to be resolved.

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 reach out to the NCBI Help Desk if they have any questions regarding their information or have concerns that need to be resolved.

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 data integrity audits are conducted by BLAST Administrative Staff.

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.

Individuals who sign up for email announcements are verified through a confirmation email. Individuals only have access to their PII.

System administrators are approved based on their technical/functional role in administering, developing, and supporting the daily job functions of BLAST.

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.

Access to PII is assigned to personnel based upon current job responsibilities. An IAM 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 and privacy 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).

N/A

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 NIH Records Retention Schedule.

Item 10-101 - Administrative records maintained in any agency office.
Administrative records maintained in any agency office. Records accumulated by individual offices that relate to routine day-to-day administration and management of the office rather than the mission-specific activities for which the office exists, excluding records scheduled elsewhere in the General Records Schedule (GRS) such as timekeeping and procurement.
Disposition: Destroy when business use ceases. DAA-GRS2016-0016-0001

Item 07-204 - System access records; Systems requiring special accountability for access; These records are created as part of the user identification and authorization process to gain access to systems. Records are used to monitor inappropriate systems access by users.
Disposition: Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use. DAA-GRS-2013- 0006-0004

Item 07-201- Systems and data security records;
These are records related to maintaining the security of information technology (IT) systems and data.
Records outline official procedures for securing and maintaining IT infrastructure and relate to the specific
systems for which they were written. This series also includes analysis of security policies, processes, and
guidelines, as well as system risk management and vulnerability analyses.
Disposition: Destroy 1 year(s) after 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. 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: System administrators are approved by for access based on their technical/functional role in administering, developing, and supporting BLAST's daily job functions, and BLAST administrators perform periodic reviews to assure users adhere to system policies.

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 NLM Data Center 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.

Identify the publicly-available URL:

https://blast.ncbi.nlm.nih.gov/Blast.cgi

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?

Yes

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

Yes