NIH Office of Research Services (ORS)
Division of Personnel Security
System Access Request

USER AGREEMENT

PRIVACY ACT ADVISTEMENT: The Background Investigation Tracking System (BITS), Cross Match WEBS, Health and Human Services (HHS) Identity Portal, Enrollment Workstation (EWS) and Issuance Workstation (IWS), and any current or future peripherals or components, are U.S. Government Systems which contains Personally Identifiable Information (PII) which is protected under the Privacy Act of 1974[1]. Any unauthorized disclosure of the information contained in this electronic system should be reported to the Division of Personnel Security and Access Control (DPSAC).

AUTHORITY: Executive Order 10450[2], 9397[3] and Public Law 99-474 the Computer Fraud and Abuse Act[4]

PRINCIPLE USES: Recording of user information, user requested access and user signature; signifying agreement to follow the DPSAC Systems Rules of Behavior (ROB), and for the purpose of validating the trustworthiness of individuals requesting access to the HHS Identity Portal, EWS/IWS, NIH Background Investigation Tracking System (BITS) application and/or associated components, peripherals and information contained therein.

ROUTINE USES: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act[5], these records or information contained therein may specifically be disclosed outside NIH as a routine use pursuant of 5 U.S.C. 552a(b)(3)[6] as follows: To a Federal, State, or local law enforcement agency when your agency becomes aware of a violation or possible violation of civil or criminal law; to the Department of Justice (DOJ) for the purpose of representing NIH or HHS in any pending or potential litigation to which the record is pertinent; to the Merit Systems Protection Board for the purpose of litigation or investigation of alleged or possible prohibited personnel practices; to a Federal agency when conducting an investigation or inquiry for security audit reasons; or the General Services Administration in connection with its responsibilities for records management. These records may be furnished to the NIH Intelligence Director, Department of Health and Human Services (HHS) Counterintelligence and/or Insider Threat Team as part of the eligibility determination process.

CONFIDENTIALITY: Records contained within HHS Identity Portal, EWS/IWS, BITS, or any of the BITS peripherals or components, may fall under the ownership of non-NIH/HHS government entities. Unauthorized distribution, reproduction, modification or deletion of any applicant, employee or student information outside the intended and approved use is strictly prohibited. Instructions for distribution, reproduction and handling of these records must adhere to DPSAC policies. Records are stored for the explicit purpose of determination of eligibility and should be destroyed after an eligibility has been rendered and the data is no longer needed in accordance to the HHS System of Records Notice (SORN) and HHS retention schedule and BITS Record Retention Policy (dated 06262020). Reproduction or distribution of information or records contained within BITS, or any of the BITS peripherals or components, to non- NIH/HHS entities or individuals who do not have a need to know for the purposes of eligibility determination is strictly prohibited without the consent of the BITS data owner and record owner. Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.

DISCLOSURE: Communications using, or data stored within HHS Identity Portal, BITS, or any of the BITS peripherals or components, are subject to routine monitoring, interception, search, and may be disclosed or used for any U.S. Government-authorized purpose. This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests and may not be used for your personal benefit or privacy.

Requestor Information

Disclosure of this information is voluntary; however, failure to provide the requesting information will impede, delay or prevent further processing of this request.

Legal Name (Last, First, Middle):	**NIH (HHS) ID:**
Email:	**Phone:**
Classification: ☐ **Federal Employee** ☐ **Contractor** ☐ **Vendor**	**Department / Division:** ☐ **Division of Personnel Security** ☐ **Division of Police** ☐ **Identity Access Management** ☐ **Insider Threat** ☐ **Other**
Access Type: ☐ **New Account** ☐ **Modify Account** ☐ **Delete Account**	

Requester Justification

Provide a detailed description of the tasks / process to be performed. If multiple permissions required, list them and provide a justification for each permission needed (i.e. if you need multiple permissions in SCMS).

Requestor Agreement

I have read the DPSAC Rules of Behavior (ROB), dated January 31, 2021 and understand and agree to comply with its provisions. I understand that violations of the DPSAC ROB or information security policies and standards may lead to disciplinary action, up to and including termination of employment; removal or debarment from work on Federal contracts or projects; and/or revocation of access to Federal information, information systems, and/or facilities; and may also include criminal penalties and/or imprisonment. I understand that exceptions to the DPSAC ROB must be authorized in advance in writing by the OPDIV Chief Information Officer or his/her designee. I also understand that violation of laws, such as the Privacy Act of 1974, copyright law, and 18 USC 2071, which the DPSAC ROB draw upon, can result in monetary fines and/or criminal charges that may result in imprisonment.

By signing this form, I certify that I have read and understand the User Agreement ("Agreement") and that I am solely responsible for the proper use and protection of the information contained within ANY of the HHS, NIH or DPSAC systems. I further understand that my failure to comply with the requirements of this Agreement may result in one or all the following actions: Immediate revocation of system access and / or user privileges; disciplinary action as well as civil and criminal penalties.

Requestor's Signature	**Date**

Manager Approval

By signing this form, I approve this employee, contractor or vendor, for access requested on the following pages. I also certify that the requestor has the appropriate level of background investigation favorably completed at the correct level for access being requested.

Manager's Signature	**Date**

Personnel Security Verification

User has the appropriate level of investigation and a favorable adjudication, as required by the system module/function requested on Page 4 of this form

Investigation Type	Investigation Closed Date	Adjudication Date

OpDiv Security Administrator Signature	Date

System Owner Certification

Requestor is ☐ **Approved** or ☐ **Denied** and granted access to the systems requested.

System Owner's Signature	Date

Denial or Access Modification Reason

.Endnotes

[1] "The Privacy Act of 1974." *National Archives and Records Administration*, National Archives and Records Administration, www.archives.gov/about/laws/privacy-act-1974.html.

[2] "Executive Orders." *National Archives and Records Administration*, National Archives and Records Administration, www.archives.gov/federal-register/codification/executive-order/10450.html.

[3] *EXECUTIVE ORDER 9397 NUMBERING SYSTEM FOR FEDERAL ACCOUNTS RELATING TO INDIVIDUAL PERSONS*, www.ssa.gov/foia/html/EO9397.htm.

[4] Hughes, William J. "H.R.4718 - 99th Congress (1985-1986): Computer Fraud and Abuse Act of 1986." *Congress.gov*, 16 Oct. 1986, www.congress.gov/bill/99th-congress/house-bill/4718.

[5] *Govinfo*, www.govinfo.gov/app/details/USCODE-2010-title5/USCODE-2010-title5-partI-chap5-subchapII-sec552a.

[6] Ibid