

US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/05/2025

OPDIV:

NIH

Name:

DPCPSI Dashboard

PIA Unique Identifier:

P-6817699-317455

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

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

The only changes since the last assessment is that SharePoint has moved from the 2016 version to the 2019 version.

Describe the purpose of the system.

The Division of Program Coordination, Planning, and Strategic Initiatives (DPCPSI) Dashboard is a SharePoint 2019 based system housed within the National Institutes of Health (NIH) that provides administrative and programmatic information, electronic workflow, intranet, and document storage to/for Division employees, volunteers, contractors, and others under the Division's Standard Administrative Codes (SAC) codes. Other site collections of the SharePoint environment provide collaboration features to the Institutes and Centers (ICs) and a portal where ICs can request co-funding from the Division. The Dashboard is comprised of a variety of network, application, and web servers. A limited amount of Personally Identifiable Information (PII) is stored in the Dashboard.

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

Dashboard stores administrative management, planning and budgeting, human resource management, supply chain management, controls and oversight, general information, and internal risk management and mitigation information. Specific examples of PII include: names, the Health and Human Services (HHS) ID, Capital Human Resource (EHRP) number, phone numbers, building and office number, resume, email address, salary and past awards information and reimbursement information from Status of Funds Internet Edition (SOFiE), and information on whether the employee is "Active" (a current employee of the Division) or "Terminated" (a past employee of the Division). SOFiE maintains its own Privacy Impact Assessment, with all legal authorities documented. The Dashboard also has a position number (called a SharePoint job code) that tracks which individual(s) have filled specific positions in the Division.

Users log in to the Dashboard using the NIH Identity, Credential, and Access Management Services: Identity Management Services (IMS), formally known as the Active Directory (AD), which maintains its own unique PIA. The purpose of the IMS 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 IMS collects unique user credentials and stores them in an encrypted format. The IMS 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.

The Division of Program Coordination, Planning, and Strategic Initiatives (DPCPSI) Dashboard is a SharePoint 2016 based system housed within the National Institutes of Health (NIH) that provides administrative and programmatic information, electronic workflow, intranet, and document storage to/for Division employees, volunteers, contractors, and others under the Division's Standard Administrative Codes (SAC) codes. Other site collections of the SharePoint environment provide collaboration features to the Institutes and Centers (ICs) and a portal where ICs can request co-funding from the Division. The Dashboard is comprised of a variety of network, application, and web servers. A limited amount of Personally Identifiable Information (PII) is stored in the Dashboard.

Dashboard stores administrative management, planning and budgeting, human resource management, supply chain management, controls and oversight, general information, and internal risk management and mitigation information. Specific examples of PII include: names, the Health and Human Services (HHS) ID, Capital Human Resource (EHRP) number, phone numbers, building and office number, resume, email address, salary and past awards information and reimbursement information from Status of Funds Internet Edition (SOFiE), and information on whether the employee is "Active" (a current employee of the Division) or "Terminated" (a past employee of the Division). SOFiE maintains its own Privacy Impact Assessment, with all legal authorities documented. The Dashboard also has a position number (called a SharePoint job code) that tracks which individual(s) have filled specific positions in the Division.

Users log in to the Dashboard using the NIH Identity, Credential, and Access Management Services: Identity Management Services (IMS), formally known as the Active Directory (AD), which maintains its own unique PIA. The purpose of the IMS 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 IMS collects unique user credentials and stores them in an encrypted format. The IMS is 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.

Name
E-Mail Address
Mailing Address
Phone Numbers
Financial Accounts Info
Employment Status
Resumes
HHS ID Number
EHRP Number
SharePoint Job Code

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

Employees
Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

Resumes are used for two purposes: 1) to maintain contract files, and 2) to compile briefing documents for new, senior level NIH staff (e.g., DPCPSI Office Directors) who need information about their staff, work experience, and skills. Financial information (e.g., salary and past awards) and the EHRP number populate the awards form and provide programmatic management to the administrative officers and Division Directors. The HHS ID is used as the unique identifier between systems to tie together data from the different systems. Other information, such as email, office number, and phone number are used to create staff rosters for internal use only. No information is shared outside of DPCPSI or The Office of the Director (OD) Executive Office (for approval paperwork). The SharePoint job code is a position-specific number that helps to ensure that the division stays within its federal employee ceiling.

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

On occasion, other ICs or OD offices ask for a demo of the DPCPSI dashboard to see if the functionality could be used in other areas of the NIH. The demo would include showing employee lists, which contain user names, HHS ID, phone number, and office number.

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

5 U.S.C. 1302, 2951, 4118, 4and 506. 44 U.S.C. 3101and 3102.
Budget and Accounting Act of 1950 (Pub. L. 81-784)
44 U.S.C 3101 & 3102.

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.

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Email

Online

Identify the OMB information collection approval number and expiration date

Not Applicable. An OMB collection approval number is not needed as the Dashboard only uses the PII of federal employees for internal use only.

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.

The collection and use of employee information gathered from system interfaces and manually entered by Human Resources (HR) or administrative staff is required to produce HR and HR-related reporting. Some of these system interfaces, such as the NIH Enterprise Directory (NED) require individuals to give personal information upon hiring. Notice of information collection is given at the time of acceptance of employment at the NIH, either as federal employees or direct contractors. All systems that interface with DPCPSI Dashboard maintain their own PIAs, with legal authorities documented.

Additionally, the Dashboard has a Privacy Act Statement in the footer to notify users of the uses and their rights under the Privacy Act.

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 collection and use of employee information gathered from system interfaces and manually entered by HR staff is required to produce HR and HR-related reporting. Some of these system interfaces, such as the NIH Enterprise Directory (NED) require individuals to give personal information upon hiring. Notice of information collection is given at the time of acceptance of employment at the NIH, either as federal employees or direct contractors. All systems that interface with DPCPSI Dashboard maintain their own PIAs, with legal authorities documented.

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

Project staff send all system users notices when major changes to the system occur. Notices are in the form of email. When a user identifies information for updating, they approach their Administrative Officer about the change. At times, they are directed to update their own information in NED. On rare occasion, the administrative officer asks the Dashboard owner or developer to make an update (such as changing a SharePoint job code).

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.

The system owner uses the Dashboard Reports module to monitor the system, the data collected, and discrepancies. The system has auditing and alert features, so the system owner is notified of conflicting information in the system (such as discrepancy reports).

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

The system owner uses the Dashboard Reports module to monitor the system, the data collected, and discrepancies. The system has auditing and alert features, so the system owner is notified of conflicting information in the system (such as discrepancy reports).

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.

The Dashboard uses strict rules to determine which user(s) access PII. General users can see basic contact information about staff, seating assignment, email, and contacting information.

Administrative Officers and the Dashboard administrators and developers see the most PII as part of organizational management and system stewardship. Office Directors have access to all information about their staff in that particular SAC code for organizational management. Division Directors cannot see other offices' information, other than staff rosters for other offices.

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.

The Dashboard assigns security roles to users based on 1) SAC code, 2) NED org title (e.g., Administrative Officers (AO)s get the AO role; Office Directors get the Office Director role). All others, other than the administrators and developers, are granted the general user role based on SAC code.

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).

Not applicable

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 maintained within DPCPSI Dashboard for a time of no less than two years after an award is approved or disapproved, whichever is later, in accordance with NARA record retention schedule: 06-203, Employee incentive award records: DAA-GRS-2017-0007-0003.

Records are maintained within DPCPSI Dashboard until business needs cease, in accordance with NARA record retention schedule: 10-101, Common Office Records: DAA-GRS-2016-0016-0001.

Records are maintained within DPCPSI Dashboard for a time of no less than three years but longer retention is authorized, in accordance with NARA record retention schedule:

05-101, Financial management and reporting administrative records:DAA-GRS-2016-0013-0001.

Records are maintained within DPCPSI Dashboard business needs cease but longer retention is authorized, in accordance with NARA record retention schedule: 05-104, Financial transaction records related to procuring goods and services, paying bills, collecting debts, and accounting: DAA-GRS-2013-0003-0002.

Records are maintained within DPCPSI Dashboard for a time of no less than 3 years after records related to the coordination, implementation, execution, monitoring, and completion of grant and cooperative agreement programs in accordance with NARA record retention schedule: 09-201, Facility, space, vehicle, equipment, stock, and supply administrative and operational records: DAAGRS-2016-0011-0001.

Records are maintained within DPCPSI Dashboard for a time of no less than three years after business use has ended or is superseded in accordance with NARA record retention schedule: 08-102, Records management program records: DAA-GRS-2013-0002-0007.

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

Administrative Controls: The Division assigns individuals as administrators only with need-to-know access to update the system, develop the applications, and perform audits. In addition, the system owner maintains non-disclosure agreements of every direct contractor.

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 organizational title. 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 OD Office for Information Technology 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.