US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

02/25/2025

OPDIV:

ACF

Name:

OPRE Portfolio Management System (OPS)

PIA Unique Identifier:

P-9995557-932032

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Implementation

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?

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 OPRE Portfolio Management System (OPS) aims to provide greater visibility into research, evaluation, and data activities, while streamlining budget and administrative tasks. The system will offer the following functionalities:

Budget Planning & Management: Enter and manage funding, budgets for agreements, file storage, and automate approval workflows.

Procurement Management: Track and manage procurement activities, requisitions, milestones, and customize workflows.

Invoice Management: Enter and manage invoices, track spend against budgets, and store related files.

Project Catalog: Create and manage project information, linking them to financial agreements and

portfolios.

Staffing Management: View and manage staff assignments.

Reporting & Data Exports: Export data for various workflows, including syncing with external systems and preparing reports.

Data Importing/Uploading: Bulk import data from spreadsheets or CSV files.

User & Permissions Management: Control system access based on roles and job functions.

OPS has been chosen as the system acronyms instead OPMS for simplicity and user-friendliness, following stakeholder agreement and user research.

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

The information collected and maintained in OPS consists of data elements that are collected from other agency information systems and data that is directly entered from OPRE internal authorized users. These users have a job function that requires access to OPS and have undergone relevant training and requirements to procure OPS access from a standardized documented process. Further information on requirements for OPS access can be found within the System Security Plan (SSP) and its appendices.

The agency information systems that provide data include: the Unified Financial Management System (UFMS), Grant Solutions, Program Support Center (PSC) Revenue, Invoices, and Cost Estimates Systems (PRICES), PSC Acquisitions, Purchase Request Information System (PRISM), and Health and Human Services (HHS) Financial Business Intelligence System (FBIS). However, there are no direct relationship between OPS and the systems mentioned above. Authorized users log into each of the systems and copies relevant financial information including document number, dollars, and dates into OPS. Information is only collected or received electronically from these systems and entered manually for additional processing into OPS. Even though there is manual input of some datasets and there does exist some automated validation of data in some scenarios, manual human review and quality check is still required in appropriate scenarios. In example, financial agreements and the datasets contained therein undergo multiple stages of review and approval by designated personnel within the corresponding OPRE division before proceeding through various stages of the agreement’s lifecycle.

The data elements and supporting documents that are maintained and stored in OPS include:

Purchase Orders:

Purchase requisition number, line number, shipment number, dollar amount, funding appropriation, date planned and responsible Contracting Officer Representative (COR).

Invoice and payment details (contract/task order number, invoice number, invoice date, detailed work performed, period of performance, associated costs, payment date

Automated Clearing House (ACH) transaction number of payment) for all OPRE financial activity, Direct Obligation document numbers copied from UFMS and FBIS

Procurement fee and associated support fee amounts

Grantee names, grant number, and grant amount copied from Grant Solutions

Users' names and government email addresses

COR certificates (names, certification level, and certificate expiration date) may be stored as attachments to acquisition requests per procurement shop requirements.

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

OPRE's OPS is envisaged to empower OPRE leadership and staff with the visibility they need into the office's research, evaluation, and data activities, as well as streamline budget and administrative tasks.

Presently, OPRE does not have a centralized system to collect and store information about the projects that staff are working on. Most budget-related information is stored in OPRE's Management & Accounting for Projects System (MAPS), but project-related information (e.g., research topic, method, population, etc.), staffing information, and some budget information are stored in varied, individual spreadsheets.

The high-level purpose for OPS includes budget planning and management, procurement management, invoice oversight, project cataloging (including addressing the need described in the previous paragraph), and staffing management. In addition, the application will facilitate reporting & data exports as well as importation of required data.

OPS consists of multiple infrastructure components including persistent storage (including a Relational Database Management System), containerized representational state transfer, application programming interface (API) and a static frontend. OPRE has procured a Microsoft Azure cloud tenant, hosted within the ACF Tech organization to serve OPS in the traditional commercial regions.

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
Financial Accounts Info
Certificates

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

Employees
Business Partner/Contacts (Federal/state/local agencies)
Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

100-499

For what primary purpose is the PII used?

The overall purpose of OPS is to track OPRE's funding and the vehicle through which that money was spent (e.g., contract).

The PII about the system users (e.g., budget staff, system administrators etc.) is collected and used to manage their accounts and authenticate them during the log in process.

The Contracting Officer Representative (COR) certificates may be attached to acquisition requests when required by the procurement shop.

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

here is no secondary use for the PII within OPS

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

5 U.S.C. 301; Departmental regulations May 5, 2024.

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

Email

Government Sources

Within the OPDIV

Identify the OMB information collection approval number and expiration date

Office of Management and Budget (OMB) information collection approval requirements are not applicable because collection from the general public is not done directly in OPS.

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.

System users are made aware of the collection of their PII upon account creation. Their name and email addresses are required values as part of the documented process to request access and users are explicitly told in that process of this data collection and storage. Vendors are made aware that PII will be collected and used through their contract with OPRE

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.

System users are technically able to opt-out of the collection of their PII, however, this would result in not being approved for OPS access which may not be allowable based on their job responsibilities. Vendors are not able to opt-out of the collection as the information collected is required by their contract with OPRE and necessary to execute invoices.

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

System users whose PII is stored within OPS (OPRE staff) will be notified by email when major

changes to how their data is used or when disclosures have occurred.

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.

System users are required to complete a mandatory ACF Cybersecurity and Privacy Awareness trainings including system-specific training on OPS User Access Administration manual prior to be granted access to the system. During these trainings, the users are told to reach out the appropriate contact point if they have any concerns with their PII being inappropriately obtained, used or disclosed.

If a vendor is concerned with how their PII is being obtained, used, or disclosed or that it is inaccurate, they can contact their Contracting Officer (CO) or COR who can route the concern to the appropriate staff within OPRE for resolution.

Should OPRE suspect or confirm that information from OPS has been obtained, used, or disclosed inappropriately they shall notify the ACF Incident Response Team to review and investigate the issue.

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

Availability: The system is hosted in Microsoft Azure which has several controls in place to assure that it remains available to users who need it. If the system does become unavailable, the data is backed up on a daily basis to a different Azure availability zone.

Integrity: The system's role-based access controls (RBAC) limit a user's ability to modify information they do not need for their project or contract. Additionally, a system log captures each update to the data, along with who made it and when, and can be reviewed if needed to confirm the integrity of the data.

Accuracy: All PII in OPS is received electronically and entered manually from other systems that are responsible for assuring the information is sufficiently accurate. Some non-PII is obtained directly from the vendor and transcribed into the system by a user. Where possible, OPS verifies that the entered information matches the expected formatting and characters. It is updated when OPRE staff learn about changes, which is sufficient for the employees and contractors using the system.

Relevancy: PII is added to OPS when an individual becomes a point of contact for one or more contracts. Once in the system, it will be updated, but old information will be maintained until a specific retention and destruction schedules is approved by NARA (currently pending).

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.

OPRE employees who oversee one or more OPRE contracts (called Project Officers) receive access to OPS and the PII associated with each contract they oversee.

OPRE employees and contractors who assist with the procurement process (e.g., the Budget Officer

and staff who help process the invoices) work with every OPRE contract and therefore receive access to OPS and the PII associated with each contract.

OPRE contractors and developers who maintain OPS IT infrastructure receive access to every OPRE contract and the associated PII in case they need to fix an issue that another user cannot resolve through the user interface.

Before any user receives access to OPS, (a) the director of an OPRE division must approve their access and (b) the user must complete mandatory ACF security & privacy awareness training, OPS-specific training, and any role-based training as needed.

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.

All OPS users are granted specific application access and the PII data elements strictly in accordance with ACF Tech access control policy. Allowing access to the PII data is only performed on a need to know and least privilege principle. OPS only allows authorized users that have the necessary privileges and roles to perform their assigned responsibilities including accessing of its PII.

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.

Any authorized OPRE staff granted access to OPS complete OPS-specific training prior to being granted access to the system. This would be in addition to any relevant role-based training, as well as ACF mandated security & privacy awareness training.

Describe training system users receive (above and beyond general security and privacy awareness training).

All authorized users of the system are required to take Emergency Preparedness Training, Records Management training including reading, acknowledging and adhering to the HHS/OpDiv Rule of Behavior (RoB) prior to accessing the OPS system and its data, annually thereafter and when required by system changes. In addition, all contracting officer representatives (CORs) are required to complete monthly procurement trainings and other tailored trainings specific to the role they are assigned. Users also have system documentation (e.g., user guide, help screens) available within the application.

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.

The current retention and destruction guidelines are outlined in OPS procedural documentation. At this time, all data is kept on a permanent basis for research and trend analysis purposes. The program will review the current guidelines and work together with their records liaison to create a file plan for the various records contained within OPS, including a determination on what should be temporary and what needs to be permanent.

At the end of the 5-year availability of the funding, expired budget lines are put on hold, so that Project Officers can't try to invoice against. Once Contracts are officially closed at PSC, the budgets lines and historical information can be closed and archived.

The following are OPRE Record Schedules that are used to cover all the OPS PII data retention and destruction requirements throughout the cycle. These include, DAA-0292-2016-0014 2.1, DAA-0292-2016-0014 2.2, DAA-0292-2020-0005.

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

The system is categorized as Federal Information Processing Standard (FIPS) 199 - Moderate. It has numerous policies and procedures to govern and protect the data it stores.

Administrative- Access to the system is restricted by Personal Identity Verification (PIV) card and Personal Identity Number (PIN) unless special limited exceptions have been granted. Access to administrative functions is limited to those who need access as part of their job function. The delineation between users and administrators is controlled using role-based access. Users are given access only to the part of the system that they need access to, based on their project and/or contract. All role assignments are reviewed and approved by OPRE federal division directors and the user is required to complete OPS-specific training prior to being granted their account.

Technical- The system is behind a firewall that restricts access to only the functions necessary for operation. Standard denial of service, antivirus, and patching/remediation is in place to prevent unauthorized access. Multi-factor authentication is implemented for all users. Should unauthorized access occur, the incident response process will be activated to resolve the incident.

Physical- The system is housed entirely in the Azure East region, that is also certified by the Federal Risk and Authorization Management Program (FedRAMP) for High systems. Access to the data center is restricted to the Cloud Services Provider’s authorized employees, vendors, and contractors.