PTA / PIA: OS - EFlow - QTR2 - 2026 - OS3427350

Created Date: 5/15/2026 5:06 PM Last Updated: 5/29/2026 5:05 PM

General Information

PTA / PIA Name:	OS - EFlow - QTR2 - 2026 - OS3427350	**PTA / PIA ID:**	4488151
Component Name:	OS - OS - Electronic Workflow	**ATO Boundary Name:**	Electronic Workflow
Overall Status:	Complete	**# of Days - Open:**	36
Submitter:		**Submit Date:**	5/11/2026
Next Assessment Date:	05/28/2029	**Expiration Date:**	5/28/2029
Office:		**OpDiv:**	OS
Security Categorization:	Moderate		
Make PIA available to Public?:	Yes	**PIA Required:**	Yes

General 01:	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
General 02:	Is this a FISMA-Reportable system?	Yes
General 03:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	Yes
General 04:	ATO Date or Planned ATO Date.	1/31/2028
General 05:	Is the system or electronic information collection, agency or contractor operated?	Contractor
History Log:	View History Log	

Privacy Threshold Analysis

Privacy Threshold Analysis

PTA 01:	Point of Contact (POC) Name	Ricky Ford
PTA 01A:	POC Title and Organization	Information Systems Security Officer, Office of the Secretary (OS), Office of the Chief Information Officer (OCIO), Office of Information Security (OIS)
PTA 01B:	POC Email Address	ricky.ford@hhs.gov
PTA 01C:	POC Phone Number	301-525-7322
PTA 02:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)

PTA 02A:	Describe in further detail any changes to the system that have occurred since the last PIA.	Electronic Workflow (eFlow) service functionality was updated to incorporate functions from the Cost Allocation Management Information System (CAMIS). The functions were added to eFlow to incorporate CAMIS functions provided to users. These functions include: 1) Rate Agreement Generation, 2) an employee staff/time module, and 3) a report generation module. Multi-factor authentication (MFA) using a PIV card was implemented on eFlow.
PTA 03:	Is the data contained in the system owned by the agency or contractor?	Agency
PTA 04:	Please give a brief overview of the purpose of the system by describing what the functions of the system are and how the system carries out those functions in support of HHS.	Electronic Workflow (eFlow) is a document imaging system used to scan invoices, as well as route invoices to designated Financial Management Portfolio (FMP) users who will approve or reject invoices in the Unified Financial Management System (UFMS). UFMS applications are supporting common processes for financial operations of HHS. UFMS has its own separate privacy impact assessment (PIA). eFlow is an intermediary system that forwards scanned invoices to UFMS for payment processing. The application is used for capturing of paper invoices via scanned image, indexing, and workflow with Accounts Payable staff in Accounting Services (AS), reporting/status of documents in workflow, and creation/output of vendor letters. The type of invoices scanned into eFlow are commercial vendor related invoices such as (FedEx, Canon, UPS,) etc. The scanning of invoices is the process of uploading the invoice documents into the system for review and payment by the Accounts Payable staff. The approval of an invoice occurs in the review process in eFlow by staff, where the vendor invoice information is compared with the information in the UFMS, if vendor information is in agreement with the UFMS, the invoice is approved for payment. The rejection process occurs when the vendor invoice scanned into eFlow, is reviewed by Accounts Payable staff, and the information on the vendor invoice does not match what's in the UFMS. The invoice is rejected and sent back to the vendor for updated vendor information.
PTA 05:	List and/or describe all the types of information that are collected, maintained, and/or shared by the system regardless of whether that information is PII and how long that information is stored.	eFlow contains financial information about vendors such as: vendor name, invoice numbers, account numbers, account routing numbers, and vendor business address as a scanned image of a hard-copy invoice. The vendor information stored in eFlow can be retrieved by vendor name, address, invoice number, and date of which the invoice was scanned/uploaded into the system. The invoice information used is already present on the invoices from vendors before they are scanned by Accounts Payable employees and direct contractors from AS. The information may contain personally identifiable information (PII) if vendors are individuals. The information is stored indefinitely.

PTA 05A:	Are user credentials used to access the system?	Yes
PTA 05B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS/OpDiv PIV Card
PTA 06:	Describe why each type of information is collected, maintained, and/or shared by the system. Specify what information is collected about each category of individual.	eFlow contains information that can be found on the invoices provided by vendors for payment tracking in UFMS. Vendors (including any individuals) complete and submit this information in order to receive compensation. It contains financial information about vendors such as: vendor name, invoice numbers, account numbers, account routing numbers, and vendor business address as a scanned image of a hard-copy invoice. The vendor information stored in eFlow can be retrieved by vendor name, address, invoice number, and date of which the invoice was scanned/uploaded into the system. The invoice information used is already present on the invoices from vendors before they are scanned by Accounts Payable employees and direct contractors from AS. The information may contain PII if vendors are individuals. EFlow does not share PII outside of the Office of the Secretary (OS).
PTA 07:	Does the system collect, maintain, use, or share PII?	Yes
PTA 08:	Does the system include a website or online application?	No
PTA 14:	Does the system have a mobile application?	No
PTA 20:	Are any third-party websites or applications (TPWA) associated with the system?	No
PTA 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

Privacy Impact Assessment

Privacy Impact Assessment

PIA 22:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Identifying Numbers Financial Account Information (e.g., account numbers, credit card numbers) Biographical Information Name Contact Information Mailing Address (Business) Other Other
PIA 22A:	Identify the "other" type(s) of personally identifiable information (PII) not mentioned in the above list.	Invoice number, vendor account number, vendor name, vendor account routing number, vendor business address
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Employees/HHS Direct Contractors Vendors/Suppliers/Third-Party Contractors (Contractors other than HHS Direct Contractors)
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	100 – 499

PIA 25:	For what primary purpose is the PII used?	The primary purpose for using PII in the eFlow system is to allow the employee or direct contractor to properly identify those vendor invoices for payment using (Vendor name, Address, Invoice Number, and Date). Within the eFlow system as a part of the business review process the employee/ direct contractor use these element captured on the invoices scanned into the system. In addition the Accounting Services (AS), Accounts Payable uses the information to generate internal reports to learn the status of the vendor invoices as it relates to the payment process.
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	None
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	eFlow captures images of invoice information. This collection is covered by other systems, such as the Unified Financial Management System (UFMS), which utilizes forms required under 31 USC 3322, 31 CFR 209 and/or 210
PIA 29:	Are records in the system retrieved by one or more PII data elements?	Yes
PIA 29A:	Please specify which PII data elements are used to retrieve records.	PII data elements used to retrieve records are vendor name, address, invoice number, and date.
PIA 29B:	Provide the number, title, and URL of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or indicate whether a new or revised SORN is in development.	09-90-0018 Fin. Trans. of HHS Acct and Fin. Off
PIA 30:	Identify the sources of PII in the system.	Government Sources Within the OPDIV Non-Government Sources Private Sector
PIA 31:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA 31B:	Explain why an OMB information collection approval number is not required.	Not Applicable
PIA 32:	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	No
PIA 33:	Is the submission of PII by individuals voluntary or mandatory as defined in the Privacy Act?	Voluntary
PIA 34:	Describe the method in place to notify and obtain consent from individuals whose PII will be collected. If no prior notice is given or consent cannot be obtained, explain why.	In order for a vendor to be compensated for services that have been provided, they must first be registered in the System for Award Management (SAM). Once registered that information is uploaded into UFMS. The EFlow system is an intermediary system that forwards scanned invoices (provided by the vendors) to UFMS for payment processing. As a result, vendors have the opportunity to opt-in to the collection of information in order to receive payment, hence no need to provide an opt-out.

PIA 35:	Describe the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection). If they cannot be notified or have their consent obtained, explain why.	No major changes are anticipated that would affect individuals' rights or interests. If this were to occur, HHS would be able to contact the individual using the contact information provided, and the System of Record Notice (SORN) would be updated appropriately.
PIA 36:	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. If no process exists, explain why not.	Individuals may contact the Program Support Center (PSC) Privacy Act Officer if they believe their information has been misused. The vendor could also work through the Computer Security Incident Response Center (CSIRC) or other privacy and security staff.
PIA 37:	Describe the process in place for periodic reviews of the system to ensure the integrity, availability, accuracy, and relevancy of the PII in the system. Please address each element in your response. If no processes are in place, explain why not.	eFlow is updated with a manual feed from the UFMS that updates the commercial vendor information. UFMS is the financial system of record and the use of any PII is transactional.
PIA 38:	Identify who will have access to the PII in the system.	Users Administrators Developers Contractors
PIA 38A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA 38B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes
PIA 39:	Provide the reason why each of the groups identified in 38 needs access to PII.	Users need to perform data/report validation, administrators need to perform application and user maintenance, developers need to perform application maintenance, contractors perform application and data maintenance.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	All eFlow employees are provided a user account to access the eFlow system. For a user such as (administrators, developers) to gain elevated access to PII information within the system, the employee's supervisor must submit a request to have an employee's permissions elevated in eFlow to access PII data.
PIA 41:	Describe the technical methods in place to allow those with access to PII to access only the minimum amount of information necessary to perform their job.	System administrators and developers have privileged access to eFlow while users have regular access based on their roles and responsibilities.
PIA 42:	Identify the general security and privacy awareness training provided to system users (system owners, managers, operators, contractors and/or program managers) to make them aware of their responsibilities for protecting the information being collected and maintained.	Financial Management Portfolio (FMP) employees and contractors are required to complete the annual HHS Privacy Awareness and Information System Security Awareness Training.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	All individuals with access to eFlow must accept and adhere to the HHS-Rules of Behavior that appears on the login page for the eFlow system

PIA 44:	Describe the process and guidelines in place for the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).	General Records Schedule (GRS) 1.1 item 10 - Financial transaction records. Temporary. Destroy 6 years after final payment or cancellation, but longer retention is authorized if required for business use. DAA-GRS- 2013-0003- 0001. GRS Item 3.1 item 10 - Infrastructure project records. Temporary. Destroy 5 years after project is terminated, but longer retention is authorized if required for business use. DAA-GRS- 2013-0005-0006.
PIA 45:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.	Technical and Physical controls are in place to ensure the security of the information. These include an up-to-date System Security Plan, Contingency Plan, regular off site backup of the data, and yearly security awareness training for all personnel. Specific protection for PII include: 1- Electronic data is password protected 2- Access to electronic data is role-based 3- Documents are locked in file cabinet accessible only to management and administrators

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	5/14/2026
Privacy Analyst Review Comments:	This PIA is ready for your review. All necessary questions have been answered. Thank you, Jon	**# of Days - PA Review:**	3

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	5/15/2026
SOP Review Comments:		**# of Days - SOP Review:**	1

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	5/18/2026
Agency Privacy Analyst Review Comments:	Reviewer: Crystal Bland 5/18/2026 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	3

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	5/29/2026
SAOP Review Comments:		**# of Days - SAOP Review:**	11

SAOP Signature

Date	User	Type	Name	Original Value	New Value
5/29/2026 2:53 PM	BAUR, VANESSA	Signature	SAOP (Email PIN)		Content Signed

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
No Records Found				