Privacy Impact Assessment (PIA): OS - EFlow - QTR1 - 2020 - OS503829

Date Signed: 1/24/2020

Acronyms

ATO - Authorization to Operate
CAC - Common Access Card
FISMA - Federal Information Security Management Act
ISA - Information Sharing Agreement
HHS - Department of Health and Human Services
MOU - Memorandum of Understanding
NARA - National Archives and Record Administration
OMB - Office of Management and Budget
PIA - Privacy Impact Assessment
PII - Personally Identifiable Information
POC - Point of Contact
PTA - Privacy Threshold Assessment
SORN - System of Records Notice
SSN - Social Security Number
URL - Uniform Resource Locator

General Information

Status:	Approved	**PIA ID:**	1113115
PIA Name:	OS - EFlow - QTR1 - 2020 - OS503829	**Title:**	OS - Electronic Workflow
OpDiv:	OS		

PTA

PTA - 1A:	Identify the Enterprise Performance Lifecycle Phase of the system	Operations and Maintenance
PTA - 1B:	Is this a FISMA-Reportable system?	Yes
PTA - 2:	Does the system include a website or online application?	No
PTA - 3:	Is the system or electronic collection, agency or contractor operated?	Agency
PTA - 5:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
PTA - 7:	Describe in further detail any changes to the system that have occurred since the last PIA	Minor changes were applied to improve the quality of the Privacy Impact Assessment.
PTA - 8:	Please give a brief overview and purpose of the system by describing what the functions of the system are and how the system carries out those functions?	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 has its own separate privacy impact assessment (PIA). The Electronic Workflow is an intermediary system that forwards scanned invoices to UFMS for payment processing. The application is used for capture of paper invoices via scanned image, indexing, workflow with Accounts Payable staff in Accounting Services (AS), reporting/status of documents in workflow, creation and output of vendor letters. The types of invoice 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 Electronic Workflow (eFlow), is being reviewed by Accounts Payable staff, when the information on the vendor invoice does not match what's in the UFMS, at this point the invoice is rejected back to the vendor for updated vendor information.
PTA - 9:	List and/or describe all the types of information that are collected (into), maintained, and/or shared in the system regardless of whether that information is PII and how long that information is stored.	The Electronic Workflow (eFlow) system 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 the Electronic Workflow, can be retrieved by (Vendor name, Address, Invoice Number, and Date) in which the invoice was scanned/uploaded into the eFlow system. The invoice information used by eFlow is already present on the invoices from vendors before they are scanned by Accounts Payable employees and direct contractors from Accounting Services (AS). The Electronic Workflow(eFlow) does not generate any new information for dissemination. The Electronic Workflow login credentials are not stored within the system. When creating a new eFlow user profile the system relies on a link with the HHS network to establish an employees or direct contractors login credential in the Electronic Workflow system Within eFlow invoices are routed to the designated direct contractor to verify the accuracy and completeness of the vendor invoice information, the contractor will compare the information in the eFlow with the vendor information provided in UFMS, if accurate the contractor will approve the vendor invoice for payment in UFMS. The Financial system of record for the paying of vendor invoices is UFMS. The information may contain personally identifiable information (PII) if vendors are individuals. Information submission to Electronic Workflow is voluntary. The system name, Invoice Scanning & Imaging System (ISIS), was the original name of the workflow application before it was changed to Electronic Workflow.
PTA - 10:	Describe why all types of information is collected (into), maintained, and/or shared with another system. This description should specify what information is collected about each category of individual	eFlow is a document imaging system used to scan invoices, as well as route invoices to designated users who will approve or reject

		invoices in the UFMS. The Electronic Workflow is an intermediary system that forwards scanned invoices to UFMS for payment processing. The application is used for capture of paper invoices via scanned image, indexing, workbench/workflow with Accounts Payable staff in AS, reporting/status of documents in workflow, creation and output of vendor letters. The types of invoice 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 Electronic Workflow (eFlow), is being reviewed by Accounts Payable staff, where the information on the vendor invoice does not match what's in the UFMS at this point the invoice is rejected back to the vendor for updated vendor information. Electronic Workflow (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. ISIS was the original system name of the workflow application before it was changed to Electronic Workflow.
PTA - 10A:	Are records in the system retrieved by one or more PII data elements?	Yes
PTA - 11:	Does the system collect, maintain, use or share PII?	Yes
	PIA	
PIA - 1:	Indicate the type of PII that the system will collect or maintain	Name Mailing Address Financial Account Info
PIA - 2:	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 - 4:	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 eFlow system. In addition the AS, Accounts Payable uses the information to generate internal reports to learn the status of the vendor invoice as it relates to the payment process.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research)	N/A
PIA - 7:	Identify legal authorities, governing information use and disclosure	Electronic Workflow captures images of invoice

	specific to the system and program	information which collection are covered by other Systems such as the UFMS which utilizes Forms required under 31 USC 3322, 31 CFR 209 and/or 210.
PIA - 8:	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 - 9:	Identify the sources of PII in the system	Government Sources Within the OPDIV Non-Government Sources Private Sector
PIA - 9A:	Identify the OMB information collection approval number or explain why it is not applicable.	N/A
PIA - 10:	Is the PII shared with other organizations outside the system's Operating Division?	No
PIA - 11:	Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason	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.
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
PIA - 13:	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	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 Electronic Workflow 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 - 14:	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). Alternatively, describe why they cannot be notified or have their consent obtained	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 - 15:	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 - 16:	Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. Please address each element in your response. If no processes are in place, explain why not	The Electronic Workflow is updated with a manual feed from the UFMS that updates the commercial vendor information, UFMS is the financial system of record, the use of any PII is transactional.
PIA - 17:	Identify who will have access to the PII in the system and the reason why they require access	Users Administrators Developers Contractors
PIA - 17A:	Provide the reason of access for each of the groups identified in PIA-17 Users Reasoning: Data/Report validation Administrators Reasoning: Application and user maintenance Developers Reasoning: Application maintenance Contractors Reasoning: Application and data maintenance conducted by direct contractors. Others Reasoning:	
PIA - 17B:	Select the type of contractor	

PIA - 18:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII	All Electronic Workflow (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 eFlow system, the employees supervisor must submit a request to have an employee's permissions elevated in eFlow to access PII data.
PIA - 19:	Describe the technical methods in place to allow those with access to PII to only access 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 - 20:	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	Financial Management Portfolio (FMP) employees and contractors are required to complete the annual HHS Privacy Awareness and Information System Security Awareness Training.
PIA - 21:	Describe 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 - 23:	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific 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 - 24:	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
PIA - 27:	Does the website use web measurement and customization technology?	No