




Instructions

Privacy Impact Assessment (PIA)

The Privacy Impact Analysis (PIA) questionnaire is applicable to information systems which store or process privacy data. The questionnaire collects information about the types of privacy data which are stored and processed, why it is collected, and how it is handled. A PIA is required based on the results of a Privacy Threshold Analysis (PTA) questionnaire that has been completed for the information system.

Review the following steps to complete this questionnaire:

1) Answer questions. Select the appropriate answer to each question. Question specific help text may be available via the  icon. If your answer dictates an explanation, a required text box will become available for you to add further information.

2) Add Comments. You may add question specific comments or attach supporting evidence for your answers by clicking on the  icon next to each question. Once you have saved the comment, the icon will change to the  icon to show that a comment has been added.

3) Change the Status. You may keep the questionnaire in the "In Process" status until you are ready to submit it for review. When you have completed the assessment, change the Submission Status to "Submitted". This will route the assessment to the proper reviewer. Please note that all values list questions must be answered before submitting the questionnaire.

4) Save/Exit the Questionnaire. You may use any of the buttons at the bottom of the screen to save or exit the questionnaire. The 'Save and Close' button allows you to save your work and close the questionnaire. The 'Save and Continue' button allows you to save your work and remain in the questionnaire. The 'Cancel' button closes the questionnaire without saving your work.

00 Default Layout

Workflow Status:

99 Workflow Complete

PIA

General Information

PIA ID:	PIA-273	PIA Status:	Completed
Authorization Package (System Name):	Perceptive Content (PC)	This is a RPA:	No
Assessment Date:	7/8/2021	Is Latest:	Yes
FISCAL Year:	2021	PIA Required (From Authorization Package):	Yes
Final FISCAL Year:	2021	PIA Expiration Date:	7/8/2022
		Final PIA Expiration Date:	7/8/2022

Override / Reopen Explanation

Override FISCAL Year:	2021	Override PIA Expiration Date:	
Reopened Explanation:			

Other Stakeholders

Stakeholders (not in Approval Process)

System Owner (SO): Hanna, Jennifer L	Authorization Official: DelNegro, Elizabeth F
---	--

System Owner (eMail)

Name (Full)

Jennifer Hanna

Authorization Official (eMail)

Name (Full)

Elizabeth Delnegro

PIA Overview

A.System Name:	A. System, Application, or Project Name:	Perceptive Content (PC)
B.Includes:	B. System, application, or project includes information about:	Perceptive Content EP2 (previously named ImageNow), which is a product developed by Hyland Software, is the subsystem within the Ancillary Corporate Applications (ACA) at GSA. Perceptive Content serves as the Office of the Chief Financial Officer’s (OCFO) imaging/workflow solution. Perceptive Content allows users in the Payroll Services Branch, Accounts Payable and customer agencies to annotate metadata to scanned images, and search and view documents (i.e., invoices, payroll, property records, deeds, transfers) that have been scanned/stored.
C.Categories:	C. For the categories listed above, how many records are there for each?	There are 4 million records in Perceptive Content today. That number grows every day as GSA scans additional records into the system moving forward. Out of the 4 million records, the documents are classified into 30 different departments that use the system.
D.Data Elements:	D. System, application, or project includes these data elements:	Perceptive Content which is a subsystem of ACA at GSA captures the following information on these individuals by storing images of documents as well as extracting data from the documents into metadata fields in the Perceptive Content database which contains PII (Gender, Birthdate, Marital Status, Employer Identification Number, and Social Security Number)
Overview:		
PIA-0.1:	Is this a new PIA or Recertification request?	
PIA-0.1Changes:	If you are reviewing this for annual recertification, please confirm if there are any changes in the system since last signed PIA?	Yes, there are changes

Comments

Question Name	Submitter	Date	Comment	Attachment
No Records Found				

1.0 Purpose of Collection

PIA-1.1:	What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?	48 CFR 1232.7002 Invoice and Voucher review and approval “ provides for the collection of invoices for contracts and the review of these by the government. 5 CFR 792.204 - Agency responsibilities; reporting requirement. Used by the Child Subsidy Program for tracking the utilization of funds. The images in Perceptive Content are used for review and validation of the database entries in the Child Subsidy program. While an SSN may be collected as part of the invoice data, it is not explicitly required by the application. The employer identification number is requested but if vendors choose to use their SSN instead, they can enter it.
PIA-1.2:	Is the information searchable by a personal identifier, for example a name or Social Security number?	Yes
PIA-1.2a:	If so, what Privacy Act System of Records Notice(s) (SORN(s)) applies to the information being collected?	Existing SORN applicable
	PIA-1.2 System Of Record Notice (SORN) CR:	
PIA-1.2 System of Records Notice(s) (Legacy Text):	What System of Records Notice(s) apply/applies to the information?	SORN GSA/PPFM-12
PIA-1.2b:	Explain why a SORN is not required.	Perceptive Content includes individuals’™ names or other unique identifiers in conjunction with other data elements such as gender, birth date, age, marital status, spouse and dependents, home e-mail address, home address, home phone number, health records, Social Security Number, Employer Identification Number (also known as a “tax identification number”), payroll deductions, banking information, personal credit card information, and similar personal information The Perceptive Content system is referenced in SORN GSA/PPFM-12 “Perceptive Content,” available at: FR Doc No: E9-19102, Federal Register Volume 74, Number 152 (https://www.gpo.gov/fdsys/pkg/FR-2009-08-10/html/E9-19102.htm).
PIA-1.3:	Has an information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)?	No
PIA-1.3 Information Collection Request:	Provide the relevant names, OMB control numbers, and expiration dates.	There are no standard forms that collect data from the public for this system. The data stored in Perceptive Content are just scanned images or documents provided and are not forms subject to the Paperwork Reduction Act
PIA-1.4:	What is the records retention schedule for the information system(s)? Explain how long and for what reason the information is kept.	As stated in GSA PPFM-12, the data in Perceptive Content will be stored indefinitely. At a minimum NARA requires retention for at least 6 years after contracts expire for financial management records.


2.0 Openness and Transparency

PIA-2.1:	Will individuals be given notice before the collection, maintenance, use or dissemination and/or sharing of personal information about them?	Yes
PIA-2.1 Explain:	If not, please explain.	

3.0 Data Minimization

PIA-3.1:	Why is the collection and use of the PII necessary to the project or system?	The use of PII is necessary to the Perceptive Content subsystem because the subsystem captures on individuals by storing images as well as extracting data from the documents into metadata fields in the Perceptive Content database: employee by name or other unique identifier gender, birth date, age, marital status, spouse and dependents, home e-mail address, home address, home phone number, cell phone number, work phone number, health records, Social Security Number (only captured in the image, not in the database as described in Section 2.2), Employer Identification Number, payroll deductions, banking information, personal credit card information,
PIA-3.2:	Will the system, application, or project create or aggregate new data about the individual?	No
PIA-3.2 Explained:	If so, how will this data be maintained and used?	
PIA-3.3:	What protections exist to protect the consolidated data and prevent unauthorized access?	Users request access to the system using GSA's Enterprise Access Request System (EARS). EARS forces the user to specify the roles they are requesting. In Perceptive Content the roles have pre-defined drawers that they have access to. The request from the user is approved by the supervisor and the Information System Security Officer prior to a system administrator adding the user into the role requested. Approvals are only granted where the employee has a need to access the documents contained in the Perceptive Content drawers. The roles define whether the user has read-only or write privileges. The read/write privileges may change for different drawers in the system. The data is also encrypted in the DB.
PIA-3.4:	Will the system monitor the public, GSA employees, or contractors?	None
PIA-3.4 Explain:	Please elaborate as needed.	
PIA-3.5:	What kinds of report(s) can be produced on individuals?	No reporting is completed that would include PII information.
PIA-3.6:	Will the data included in any report(s) be de-identified?	No
PIA-3.6 Explain:	If so, what process(es) will be used to aggregate or de-identify the data?	
PIA-3.6 Why Not:	Why will the data not be de-identified?	No reporting is completed that would include PII information.

4.0 Limits on Using and Sharing Information

PIA-4.1:	Is the information in the system, application, or project limited to only the information that is needed to carry out the purpose of the collection?	Yes
PIA-4.2:	Will GSA share any of the information with other individuals, federal and/or state agencies, or private-sector organizations?	
PIA-4.2How:	If so, how will GSA share the information?	Perceptive Content does not share any information to any other Agencies outside of GSA.
PIA-4.3:	Is the information collected:	From Another Source
PIA-4.3Other Source:	What is the other source(s)?	Perceptive Content extracts information from internal applications that already store the data. No information is collected from any individual.
PIA-4.4:	Will the system, application, or project interact with other systems, applications, or projects, either within or outside of GSA?	Yes
PIA-4.4Who How:	If so, who and how?	Perceptive Content interacts with internal applications such as FEDPAY and Pegasys.
PIA-4.4Formal Agreement:	Is a formal agreement(s) in place?	
PIA-4.4No Agreement:	Why is there not a formal agreement in place?	

5.0 Data Quality and Integrity

PIA-5.1:	How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?	Perceptive content is not the system of record and relies on the ancillary applications that it interacts with in order to extract the information. Perceptive Content does not complete any additional validations on the data.
-----------------	--	--

6.0 Security

PIA-6.1a:	Who or what will have access to the data in the system, application, or project?	Users request access to the system using GSA's Enterprise Access Request System (EARS). EARS forces the user to specify the roles they are requesting. In Perceptive Content the roles have pre-defined drawers that they have access to. The request from the user is approved by the supervisor and the Information System Security Officer prior to a system administrator adding the user into the role requested. Approvals are only granted where the employee has a need to access the documents contained in the Perceptive Content drawers. The roles define whether the user has read-only or write privileges. The read/write privileges may change for different drawers in the system. The data is also encrypted in the DB.
PIA-6.1b:	What is the authorization process to gain access?	The request from the user is approved by the supervisor and the Information System Security Officer prior to a system administrator adding the user into the role requested. Approvals are only granted where the employee has a need to access the documents contained in the Perceptive Content drawers. The roles define whether the user has read-only or write privileges. The read/write privileges may change for different drawers in the system. The data is also encrypted in the DB.
PIA-6.2:	Has a System Security Plan (SSP) been completed for the Information System(s) supporting the project?	Yes
PIA-6.2a:	Enter the actual or expected ATO date from the associated authorization package.	9/20/2017
PIA-6.3:	How will the system or application be secured from a physical, technical, and managerial perspective?	Perceptive Content has the capability to log the following activities with regard to which users performed actions and the time of action: 1. Documents viewed 2. Printed / Emailed / Exported Documents 3. Modification of document data 4. User access to both the Perceptive Content system and documents. Audit reviews are performed at the operating system level on a frequent basis to identify any anomalies of server-level activities. The Perceptive Content application logs may be reviewed if an incident occurs. The Perceptive Content is encrypted. Data in transit is encrypted. Only users that have gone through the multi level auth are able to access the front end of the system. Only admins with the encrypted level USB auth tools are able to access the servers.
PIA-6.4:	Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII?	Yes
PIA-6.4What:	What are they?	Email alarms are sent when suspected audit levels are breached.

7.0 Individual Participation

PIA-7.1:	What opportunities do individuals have to consent or decline to provide information?	Perceptive Content collects information from internal applications that would have to have the individuals consent to providing their information on the front end of the collection process.
PIA-7.1Opt:	Can they opt-in or opt-out?	Yes
PIA-7.1Explain:	If there are no opportunities to consent, decline, opt in, or opt out, please explain.	
PIA-7.2:	What are the procedures that allow individuals to access their information?	Users request access to the system using GSA's Enterprise Access Request System (EARS). EARS forces the user to specify the roles they are requesting. All Perceptive Content roles have pre-defined drawers that they have access to. The request from the user is approved by the supervisor and the Information System Security Officer prior to a system administrator adding the user into the role requested. Approvals are only granted where the employee has a need to access the documents contained in the Perceptive Content drawers.
PIA-7.3:	Can individuals amend information about themselves?	Yes
PIA-7.3How:	How do individuals amend information about themselves?	Individuals submit the documents that are stored in Perceptive Content by the users of the system. In the event that the individual wants to see the documents related to their records, the SORN directs them to contact the Program Manager listed in the SORN. In this way, the individual can review and provide alternative information if any discrepancies exist.

8.0 Awareness and Training

PIA-8.1:	Describe what privacy training is provided to users, either generally or specifically relevant to the system, application, or project.	Training is provided by department managers on use of the system.
-----------------	--	---

9.0 Accountability and Auditing

PIA-9.1:	How does the system owner ensure that the information is used only according to the stated practices in this PIA?	Perceptive Content has the capability to log the following activities with regard to which users performed actions and the time of action: 1. Documents viewed 2. Printed / Emailed / Exported Documents 3. Modification of document data 4. User access to both the Perceptive Content system and documents. Audit reviews are performed at the operating system level on a frequent basis to identify any anomalies of server-level activities. The Perceptive Content application logs may be reviewed if an incident occurs.
-----------------	---	--