Privacy Impact Assessment
Template

Policy, E-Government and Fair Information Practices

- Version: 4
- Date: April 5, 2018
- Prepared for: USDA OCIO-Policy, E-Government and Fair Information Practices (PE&F)

United States Department of Agriculture

Privacy Impact Assessment for the Digital Record Centre for Images

March 27, 2018

Contact Point

Jason Forsberg
Iron Mountain
972 795 1339

Reviewing Official

Ivan Jackson
National Finance Center Privacy Officer
United States Department of Agriculture
(504) 426-7551

Abstract

The abstract should be a minimum of three sentences and a maximum of four, if necessary, and conform to the following format:

- First sentence should be the name of the component and system.
- Second sentence should be a brief description of the system and its function.
- Third sentence should explain why the PIA is being conducted.

The Digital Records Center for Images is a contractor system owned by Iron Mountain. The system provides document storage of legacy paper and microfiche records as well as line data feeds for the USDA National Finance Center. Employee and contractor Personally Identifiable Information is contained within the records.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

- The system name and the name of the Department component(s) who own(s) the system;
- The purpose of the program, system, or technology and how it relates to the component's and Department's mission;
- A general description of the information in the system;
- A description of a typical transaction conducted on the system;
- Any information sharing conducted by the program or system;
- A general description of the modules and subsystems, where relevant, and their functions; and
- A citation to the legal authority to operate the program or system.

Digital Record Center for Images (DRCI) is owned and operated Information Governance Digital Solutions ("IGDS") is a division of Iron Mountain. DRCI is used to provide online web-based archive and retrieval system for line data feeds and legacy microfiche and microfilm which have been converted to digital images, to the United States federal departments. IGDS provides an isolated instance of its DRCI for USDA, which supports COLD data, images, and PDF's. The system consists of web servers, Kofax systems used to scan and store the digital files, Van Dyke system to security transfer data and Content Manager OnDemand™ for robust search and retrieval functionality. Iron Mountain has the legal authority to operate the system.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

Federal employee and contractor Name, date and/or place of birth, address, personal identification number.

1.2 What are the sources of the information in the system?

Iron Mountain and DRCI do not collect any PII. Customers of DRCI determine the sources and it is documented in their Privacy Impact Statements.

1.3 Why is the information being collected, used, disseminated, or maintained?

Iron Mountain and DRCI do not collect any PII. Customers of DRCI determine the sources and reason for collection, this is documented in their Privacy Impact Statements.

1.4 How is the information collected?

Documents will be pick up or shipped from the federal agencies offices via a secure monitored transport method to designated Iron Mountain scanning facilities. They will be then scanned, indexed and loaded for viewing within 48 hours.

1.5 How will the information be checked for accuracy?

The accuracy of the data is handled by the USDA per their standard operating procedures.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

USDA is authorization to collect information is allowed by:

- *Government Paperwork Elimination Act (GPEA, Pub. L. 105-277) of 1998,*
- *Federal Register Nol. 75, No. 27 /Wednesday, February 10, 2010/Rules and Regulations*

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Privacy Risks are minimal and have been mitigated as follows:

- *Access to the system is strictly controlled and only authorized users have access. Role based access control further restricts users access to data within DRCI.*
- *HTTPS protocol and data encryption are employed.*
- *All data enters the system as a scanned image. Each image, whether it contains PII or not is encrypted when stored.*

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

The information is to be used only by the USDA for official use.

2.2 What types of tools are used to analyze data and what type of data may be produced?

None.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

N/A

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

PII enters the system as a scanned image. All images are encrypted and stored. Access to images is strictly enforced with role based access control. Iron Mountain does not review, access or read the data; it only stores it securely for access by the client at a later date.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 How long is information retained?

Data will be maintained according to the individual customer's retention policy.

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

Data will be maintained according to the individual customer's retention policy and found in their PIA.

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

There is low risk, which is mitigated by security controls that protect the data. Access to the application and any PII is limited to only those who need access. PII data is encrypted at rest and all data is encrypted in transit.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

Iron Mountain does not share any data internally.

4.2 How is the information transmitted or disclosed?

Transmission and disclosure of data is the responsibility of the customer. Iron Mountain does not transmit or disclose any data.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Access to the application is limited to only those who need the data. Customers are responsible for the security of the data they share. Refer to each customer's PIA for additional information.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose? *PII is not shared with any external organization.*

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

N/A

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

N/A

5.4 <u>Privacy Impact Analysis</u>: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

N/A

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Does this system require a SORN and if so, please provide SORN name and URL.

No.

6.2 Was notice provided to the individual prior to collection of information?

The customer is responsible for notifying individuals of collection of information. Iron Mountain does not collect information from individuals, only stores the information securely.

6.3 Do individuals have the opportunity and/or right to decline to provide information?

The customer is responsible for interacting with individuals for the collection of data.

6.4 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

The customer is responsible for interacting with individuals for the collection of data.

6.5 <u>Privacy Impact Analysis</u>: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Controls are in place by Iron Mountain to protect the data uploaded in to DRCI. The customer is responsible for providing notice to individuals. This information is documented in their PIA.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to their information?

Iron Mountain does not allow unauthorized individuals to access the system. The customer is responsible for interacting with individuals regarding access and accuracy of PII.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Iron Mountain does not allow unauthorized individuals to access the system. The customer is responsible for interacting with individuals regarding access and accuracy of PII.

7.3 How are individuals notified of the procedures for correcting their information?

Iron Mountain does not allow unauthorized individuals to access the system. The customer is responsible for interacting with individuals regarding access and accuracy of PII.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Iron Mountain does not allow unauthorized individuals to access the system. The customer is responsible for interacting with individuals regarding access and accuracy of PII.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

This is not applicable, there is no identified risk. Refer to the customer's PIA for additional information.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

All data is encrypted. Access is strictly controlled by role based access control.

8.2 Will Department contractors have access to the system?

Only authorized users will have access to Iron Mountain DRCI.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

All IRM employees with access to Iron Mountain's IT infrastructure take Iron Mountain's global privacy and/or global information security training on a yearly basis.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

In progress.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

Verification of authorized users is conducted quarterly by Iron Mountain. Only authorized users can maintain access. All user actions are logged and auditable upon request.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

All data is encrypted at rest and in transit. Each customer's PIA will provide additional measures employed to protect the information.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1 What type of project is the program or system?

Secure document storage.

9.2 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

NO.

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 "Guidance for Online Use of Web Measurement and Customization Technology" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications"?

Yes

10.2 What is the specific purpose of the agency's use of 3rd party websites and/or applications?

N/A. No third party websites or applications are being used.

10.3 What personally identifiable information (PII) will become available through the agency's use of 3rd party websites and/or applications.

N/A

10.4 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be used?

N/A

10.5 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be maintained and secured?

N/A

10.6 Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically?

N/A

If so, is it done automatically?

If so, is it done on a recurring basis?

10.7 Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

N/A

10.8 With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared - either internally or externally?

N/A

10.9 Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

N/A

10.10 Does the system use web measurement and customization technology?

N/A

If so, is the system and procedures reviewed annually to demonstrate compliance to OMB M-10-23?

N/A

10.11 Does the system allow users to either decline to opt-in or decide to opt-out of all uses of web measurement and customization technology?

N/A

If so, does the agency provide the public with alternatives for acquiring comparable information and services?

N/A

10.12 <u>Privacy Impact Analysis</u>: Given the amount and type of PII that becomes available through the agency's use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

N/A

Responsible Officials

System Manager/Owner
Maria Jolley
Associate Director of Operations
Information Technology Services Division
USDA National Finance Center

NFC Privacy Officer / ISSPM / CISO
Ivan R. Jackson
Associate Director of Information Technology Security
Information Technology Services Division
USDA National Finance Center

Approval Signature

Jason Forsberg
Senior Director, NAO Digital Solutions Operations
Iron Mountain

Michael Zurcher
Senior Director & Global Privacy Officer
Iron Mountain