PRIVACY IMPACT ASSESSMENT (PIA) FOR DOCUMENT REDACTION SOLUTION (DRS)

08/21/2024

Prepared by:

Laurence H Schecker, Associate General Counsel and Privacy Officer, USAC

Max Mansur, ISSO, USAC

Record of Approval

Document Approval	
USAC PRIVACY POC	
Laurence H. Schecker	**Senior Advisor - Associate General Counsel and Privacy Officer**
Signature DocuSigned by: Laurence Schecker 2AFA2492613041F...	**Date** 8/22/2024
Elliot S. Tarloff	**FCC Senior Agency Officer for Privacy**
Signature Signed by: Elliot S. Tarloff 9000F2444A314E2...	**Date** 8/22/2024

Version History

Date	Description	Author
3/22/2024	Initial version of document for DRS.	Melissa Khan-CTR, Donna Howell-CTR, Dominique Arroyo - CTR
4/10/2024	Break-out ATO Boundary table in Section 1.2 by Subsystem.	Melissa Khan-CTR, Donna Howell-CTR, Dominique Arroyo – CTR
6/07/2024	Clerical and formatting edits; clarity edits to Section 1.2 Tables, 1.3A-D, 1.4A, 1.6	Privacy Advisor – Katherine Morehead Senior Agency Official for Privacy (SAOP) – Elliot S. Tarloff

TABLE OF CONTENTS

Privacy Impact Assessment for Document Redaction Solution

1.1. Introduction

Section 208 of the E-Government Act of 2002[1] requires agencies to conduct a **Privacy Impact Assessment (PIA)** whenever they procure or develop an information technology system that will collect, maintain, or disseminate information about individual people. The PIA must document how the system will use information it collects about individuals and, unless it contains classified or sensitive information, it must be made available to the public. The PIA was intended to be a tool for agencies to protect personal information throughout a technology system's life cycle. The Office of Management and Budget (OMB) has commented: "*In general, PIAs are required to be performed and updated as necessary where a system change creates new privacy risks.*"[2]

The FCC is subject to the requirements of the E-Government Act and is committed to identifying and addressing privacy risks whenever it develops or makes changes to its information systems. The questions below explore important privacy issues identified in the Act and in later guidance by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST). A longer discussion of the FCC's PIA policies can be found in Chapter 9 of the FCC's Privacy Act Manual (FCC Inst. 1113.1).

System owners, in collaboration with the Information System Security Officers (ISSOs) should complete the **Initial Privacy Assessment (IPA)** prior to filling out the PIA. The USAC Privacy Officer, in consultation with the FCC Senior Agency Official for Privacy (SAOP), uses the IPA to determine whether a system will collect the kind of information that would make it subject to the requirements of Section 208 of the E-Government Act, including a PIA. A PIA should not be completed until an IPA is completed and the SAOP makes a determination that a PIA is necessary.

If you have any questions, please contact the USAC Privacy Officer at privacy@USAC.org or the FCC Privacy Team at privacy@fcc.gov.

[1] 44 U.S.C. § 3501 note.

[2] OMB Memorandum No. M-03-22 (Sep. 26, 2003), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2003/m03_22.pdf.

1.2. Authority To Operate (ATO) Boundary Overview

For each IT system that resides within the ATO Boundary, please use the table below to provide the system name, a brief description of the what the system does, whether it contains Personally Identifiable Information (PII) and a brief description of the PII (if applicable), the applicable System of Records Notice, the legal authorities to collect and maintain the PII, and whether the PII is shared with other systems (internal or external).

The Document Redaction Solution (DRS) ATO boundary consists of the following subsystems:

- DRS Engine
- DRS Rekognition
- DRS Hyperscience Application and Trainer
- DRS Appian

INFORMATION ABOUT THE SYSTEM
NAME OF THE SYSTEM APPLICATION DRS Engine
DOES THE SYSTEM CONTAIN PII? Yes.
PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE) Lifeline and ACP applicants submit to USAC various forms of eligibility evidence, which includes PII (e.g., Lifeline Application, Household Worksheet, and related eligibility evidence documents). These image-based source files containing consumers' PII are uploaded to and stored on other USAC systems. The DRS engine processes these files, and overwrites original (unredacted) documents with documents successfully redacted by DRS. The system does not extract or store PII that it processes from the source files. The PII processed by DRS include Lifeline and ACP sensitive eligibility data, which may include identification information, contact information, financial information, authentication information, demographic information, employment information, and other identifiers.
IN WHAT SYSTEM OF RECORDS NOTICE (SORN) IS THE INFORMATION CONTAINED (IF APPLICABLE)? FCC/WCB-1, Lifeline Program, 89 Fed. Reg. 28777 (Apr. 19, 2024). FCC/WCB-3, Affordable Connectivity Program, 89 Fed. Reg. 28780 (Apr. 19, 2024).
WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII? Lifeline: 47 U.S.C. §§ 151-154, 201-205, 214, 254, 403. 47 C.F.R. §§ 54.404-54.423 ACP: 47 U.S.C. § 47 U.S.C. 151-154, 201-205, 214, 254, 403; Consolidated Appropriations Act, 2021, Public Law 116–260, div. N, tit. IX, § 904, as modified by the Infrastructure Investment

and Jobs Act, Public Law 116-260, div. F, tit V, secs. 60501, 60502(a)-(b); 47 C.F.R. Part 54 §§ 54.400, 54.401, 54.404, 54.407, 54.409, 54.410, 54.417, 54.419, 54.420, 54.1600–54.1612.
DOES THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS? The DRS Engine passes source files to DRS Rekognition and DRS Hyperscience subsystems (discussed below). The system does not extract or store PII that it processes from the source files.

INFORMATION ABOUT THE SYSTEM
NAME OF THE SYSTEM APPLICATION DRS Rekognition
DOES THE SYSTEM CONTAIN PII? Yes.
PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE) PII is contained in source files that that are processed by DRS Rekognition. The system does not extract or store PII that it processes from the source files. PII may include data to be redacted and other PII data that may reside in source files, as described for the DRS Engine, above.
IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPLICABLE)? FCC/WCB-1, Lifeline Program, 89 Fed. Reg. 28777 (Apr. 19, 2024). FCC/WCB-3, Affordable Connectivity Program, 89 Fed. Reg. 28780 (Apr. 19, 2024).
WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII? Lifeline: 47 U.S.C. §§ 151-154, 201-205, 214, 254, 403. 47 C.F.R. §§ 54.404-54.423ACP: 47 U.S.C. § 47 U.S.C. 151-154, 201-205, 214, 254, 403; Consolidated Appropriations Act, 2021, Public Law 116–260, div. N, tit. IX, § 904, as modified by the Infrastructure Investment and Jobs Act, Public Law 116-260, div. F, tit V, secs. 60501, 60502(a)-(b); 47 C.F.R. Part 54 §§ 54.400, 54.401, 54.404, 54.407, 54.409, 54.410, 54.417, 54.419, 54.420, 54.1600–54.1612.
DOES THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS? No.

INFORMATION ABOUT THE SYSTEM
NAME OF THE SYSTEM APPLICATION DRS Hyperscience (Application Server and Model Trainer)
DOES THE SYSTEM CONTAIN PII?

Yes.
PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE) For Hyperscience Application, PII is contained in source files that are processed. The files are temporarily retained (for 14 days), then auto-deleted. For Hyperscience Trainer, PII is contained in source files that are retained (until replaced by new training files) to train the DRS models. Related PII may include data to be redacted and other PII that may reside in source files, as described for the DRS Engine, above.
IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPLICABLE)? FCC/WCB-1, Lifeline Program, 89 Fed. Reg. 28777 (Apr. 19, 2024). FCC/WCB-3, Affordable Connectivity Program, 89 Fed. Reg. 28780 (Apr. 19, 2024).
WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII? Lifeline: 47 U.S.C. §§ 151-154, 201-205, 214, 254, 403. 47 C.F.R. §§ 54.404-54.423 ACP: 47 U.S.C. § 47 U.S.C. 151-154, 201-205, 214, 254, 403; Consolidated Appropriations Act, 2021, Public Law 116–260, div. N, tit. IX, § 904, as modified by the Infrastructure Investment and Jobs Act, Public Law 116-260, div. F, tit V, secs. 60501, 60502(a)-(b); 47 C.F.R. Part 54 §§ 54.400, 54.401, 54.404, 54.407, 54.409, 54.410, 54.417, 54.419, 54.420, 54.1600–54.1612.
DOES THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS? No.

INFORMATION ABOUT THE SYSTEM
NAME OF THE SYSTEM APPLICATION DRS Appian
DOES THE SYSTEM CONTAIN PII? No.
PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE) DRS Appian does not capture or store PII, rather it is an end-user application to review DRS performance and transaction status and to view inappropriate documents that are identified during processing. For failed documents, DRS Appian enables approved users to view the original file (the user is taken to the document location stored on GovCloud) for exception handling. These failed documents may contain PII, but the PII is not captured or stored in DRS Appian, and there is no ability for the end user to download the original file.

IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPLICABLE)? N/A
WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII? N/A
DOES THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS? No.

A. Is this a new ATO Boundary or an existing ATO Boundary?

☒ New Boundary

☐ Existing Boundary

B. If the ATO Boundary is/will consist of cloud-based computing system(s),[3] please check the box that best describes the service USAC receives/will receive from the cloud computing provider:

☐ USAC uses provider-supported application/s on the provider's cloud network (Software as a Service or SaaS)

☒ USAC has deployed application/s on the provider's cloud network and the provider supports the applications (Platform as a Service (PaaS)) Appian Cloud

☒ USAC has deployed its own application/s on the cloud network and controls how these application/s are configured and operate (Infrastructure as a Service or IaaS)

C. If the IT systems in the ATO Boundary are in the cloud, are they FedRAMP certified?

☐ Yes, all the IT systems are FedRAMP certified

☒ No, none, or only some, of the IT systems are FedRAMP certified.

AWS Commercial Cloud, Appian Cloud, and DRS Rekognition (hosted on AWS Commercial Cloud) are FedRAMP certified.

1.3. Collection of Data

A. Please explain why it is necessary to collect PII to carry out the purpose of each of the system(s) that maintain PII within this Boundary.

[3] *See* NIST, *The NIST Definition of Cloud Computing*, Special Pub. No. 800-145 (Sep. 2011), https://csrc.nist.gov/publications/detail/sp/800-145/final.

DRS does not collect new PII. DRS will redact PII in documents already collected by existing Lifeline and ACP systems.

B. For each system within this Boundary, will this PII be collected from individuals themselves, or from third-parties? If collected from individuals themselves, link to the Privacy Act Notice[4] for each system that is included with the online or paper form the system(s) use(s) to collect the PII.

The PII resides in application and evidence documents that USAC has already obtained, or will obtain, via existing Lifeline and ACP systems.

C. What steps is USAC taking to limit the collection of PII to only that which is necessary?

DRS does not collect new PII. DRS will redact PII in documents already collected by existing Lifeline and ACP systems.

D. What steps will USAC take to make sure this PII is accurate, complete, and up-to-date?

DRS does not collect new PII. DRS will redact PII in documents already collected by existing Lifeline and ACP systems.

1.4. Use of the Data

A. Please explain the data flow, including whether the PII will be ingested from, or shared with, another system.

The DRS Engine orchestrates the following DRS transaction processing stages (with secure, bi-directional data flow):

1. **DRS Input Service** integrates with Lifeline and ACP file storage locations that contain image-based evidence documents containing PII.
2. **DRS Process Service** utilizes Amazon Rekognition for inappropriate content scans (i.e. images unrelated to a consumer's Lifeline or ACP eligibility and containing harmful content including violence or sexual imagery). If inappropriate content is detected in a source file, a record is created in DRS Appian, a separate application, and

[4] A Privacy Act Notice must inform individuals about (1) the authority to solicit information, (2) the principal purpose(s) for collecting the information, (3) the routine uses for disclosing the information, and (4) whether providing the information is mandatory or voluntary.

notifications are sent to appropriate parties to investigate and take appropriate action.

3. **Hyperscience**, a separate application, receives cleared files – i.e. those without inappropriate content – for classification based on categories of documents required by the FCC and USAC, and redaction by the DRS Process Service, which includes -
   - Automated document classification to identify document type and apply appropriate layout/rules to digitize and analyze the content.
   - Recognition and classification of PII, resulting in document type and redacted field names being written to a Redaction History table (to store the related metadata, not the redacted PII).
   - Creation of a redacted version of file in PDF format, with PII physically blocked out so it is not visible and rendered unreadable.

   The Hyperscience user interface (UI) performs other functions, including redaction model training, model quality assurance, and manual redaction processing.
4. **DRS Output Service** overwrites original unredacted document with the redacted file and manages deletion policies for the original files.
5. **DRS Reporting State** is an Appian user interface (UI) with role-based workflow and reporting to track documents throughout their lifecycle in the DRS service, provide updates on the processing status, and manage inappropriate documents identified during processing. Metadata for Inappropriate and Failed documents is linked to the source document/file by Appian for online viewing, and DRS performance metrics are aggregated and available for ad hoc and standard reporting.

B. Will the information be shared with third-parties as part of the operations of the information system (e.g., through an application programming interface or "API")?

Yes, the DRS system boundary includes AWS Rekognition service to scan original documents for inappropriate content. No data will be stored in/by the AWS Rekognition service.

C. How long will the PII be retained and how will it be disposed of?

Hyperscience Application: Will retain original files (containing PII) for up to 14 days. Per the deletion policy, at the end of this period, the files are auto-deleted from the Hyperscience Application.

Hyperscience Trainer: Will retain up to 5,000 original files (containing PII) for each Standard Document Type for model training until replaced by new model training source files. The population of files will be refreshed during model training, with a random population of new original files overwriting existing training files.

1.5. Data Security and Privacy

A. What are the system's ratings for confidentiality, integrity, and availability?

Confidentiality	**__High**	**_X__Moderate**	**___Low**
Integrity	**__High**	**_X__Moderate**	**___Low**
Availability	**__High**	**_X__Moderate**	**___Low**

B. Discuss the physical, administrative, and technical controls in place to protect the data in the system.

DRS implements controls in accordance with the USAC baseline for Moderate systems with PII. The DRS service is hosted in the USAC AWS Commercial Cloud and Appian Cloud. DRS inherits platform encryption methodologies from these two FedRAMP-certified cloud platforms. To prevent unauthorized disclosure of data, data is encrypted at rest, utilizing a FIPS 140-3 compliant industry-standard AES-256 or higher robust encryption algorithm. Data in transit is encrypted using TLS 1.2 or greater. Auditing is performed for alter database statements, database access, and modifications to database user accounts and privileges. (This is enabled within the databases in real time.) Additionally, in compliance with USAC's Information Security and Privacy Policy, auditing is conducted for high-privileged users, local direct access to the database, actions by users who have database access, data-security events, and database-management events. Monitoring of sensitive data access and updates are performed, and automated notifications are sent to inform USAC parties of exceptions and alerts. DRS application, network, operating system, and database logs are aggregated and ingested into a security information and event management tool for monitoring and reporting.

C. Does the system inherit privacy controls from an external provider? If an Interconnection Security Agreement (ISA) , Memorandum of Understanding (MOU), or similar document is in place, please summarize the privacy applicable portions of the document.

Yes. The DRS system inherits privacy controls from the USAC AppCloud system and the Appian FedRAMP SSP.

1.6. Access to the Information

A. Which types of users will have access to the PII in this information system?

Access to PII in DRS is limited to USAC users who were granted access to review original documents in source systems (described above) on a least-privilege and need-to-know basis.

B. Does this system leverage Enterprise Common Controls (ECC)?

Yes, the DRS system inherits security controls from the USAC Enterprise Common Controls (ECC) and General Support System (GSS). These systems are FedRAMP authorized.

C. Does the system leverage the FCC's Accounting for Disclosure control?

No.