PRIVACY IMPACT ASSESSMENT FOR ROBOTIC PROCESS AUTOMATION (RPA)

02/13/2023

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** 2/13/2023	
Accepted by:		
Elliot S. Tarloff		**FCC Senior Agency Official for Privacy**
Signature Elliot S. Tarloff Elliot S. Tarloff (Feb 14, 2023 15:20 EST)	**Date** Feb 14, 2023	

Version History

Date	Description	Author
02/10/2023	PIA for RPA	Laurence Schecker, Mitchell Calhoun, Max Mansur, IT Security - ISSO
02/10/2023	Revisions from FCC Privacy	Privacy Advisor – Katherine Morehead Senior Agency Official for Privacy (SAOP) – Elliot S. Tarloff

TABLE OF CONTENTS

Robotic Process Automation (RPA)

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/wp-content/uploads/2017/11/203-M-03-22-OMB-Guidance-for-Implementing-the-Privacy-Provisions-of-the-E-Government-Act-of-2002-1.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).

INFORMATION ABOUT THE SYSTEM
NAME OF THE SYSTEM APPLICATION Blue Prism
DOES THE SYSTEM CONTAIN PII? Yes.
PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE) Blue Prism sends a process questionnaire to entities, and the questionnaire calls for the submission of the full name and Engineer Certification Number of the engineers that build out program locations. Additionally, as discussed below, carriers submit evidence to HCVS to verify their claimed service offerings, and their evidence may include incidental PII, although carriers are instructed and expected to redact such information. Carriers upload the populated questionnaires, as well as their evidence which may incidentally include PII, to Box, and Blue Prism bots transmit the document to USAC's X:drive and then to HCVS. Box, USAC's X:drive, and HCVS are not within RPA's authorization boundary; Blue Prism does not store these documents.
IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPLICABLE)? Blue Prism is not a System of Records as defined by the Privacy Act. The collection of engineer contact and certification information is governed by FCC-2, 87 F.R. 52,554.
WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII? 47 U.S.C. 254; 47 CFR Part 54, Subpart D.
DOES THE COMMISSION KEEP AN ACCURATE ACCOUNTING OF DISCLOSURES FROM THE SYSTEM AS REQUIRED BY SUBSECTION (c) OF THE PRIVACY ACT? N/A. Blue Prism is not a "System of Records," as defined by the Privacy Act, 5 U.S.C. 552a(a)(5).
DOES THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS? Yes

INFORMATION ABOUT THE SYSTEM
NAME OF THE SYSTEM APPLICATION Hyperscience
DOES THE SYSTEM CONTAIN PII? Yes.
PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE) Hyperscience may incidentally collect PII. Carriers submit evidence to verify service offerings, which are digitized and stored in Hyperscience. Evidence may include carriers' customers' bills. Carriers are instructed and expected to redact any of their customers' PII from evidence prior to submitting them to HCVS. If not redacted, the PII may be incidentally collected and stored when Hyperscience digitizes the files.
IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPLICABLE)? N/A. Hyperscience is not a System of Records as defined by the Privacy Act.
WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII? 47 U.S.C. 254; 47 CFR Part 54, Subpart D.
DOES THE COMMISSION KEEP AN ACCURATE ACCOUNTING OF DISCLOSURES FROM THE SYSTEM AS REQUIRED BY SUBSECTION (c) OF THE PRIVACY ACT? N/A. Hyperscience is not a "System of Records," as defined by the Privacy Act, 5 U.S.C. 552a(a)(5).
DOES THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS? Yes

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 the they FedRAMP certified?

☒ Yes, all the IT systems are FedRAMP certified

☐ No, none, or only some, of the IT systems 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.

Via process questionnaires, RPA intentionally collects the name and Certification Number of engineers that build out program sites in order to verify the installation of broadband services. These questionnaires are not stored within RPA. Incidental PII may be collected when carriers submit evidence of their service offerings. Such evidence can include customer bills. Carriers are instructed and expected to redact all PII prior to submission, but in the case that a carrier does not redact the PII, RPA may incidentally collect PII during Hyperscience's digitization process.

[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.

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 intentionally collected PII is collected from carriers via process questionnaires. RPA may incidentally collect PII that carriers fail to redact when submitting evidence documentation to HCVS.

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

RPA collects only names and certification numbers from engineers (via a process questionnaire) which are necessary data elements to verify the submission information. Carrier are instructed and expected to redact any of their customers' PII from evidence documentation, prior to submitting them to HCVS. If not redacted, the PII may be incidentally collected when the files are digitized by Hyperscience.

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

Carriers are responsible for ensuring the accuracy of any PII incidentally included in their submissions.

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 data flowing in and out of the RPA boundary consists of various file types and coordinates. RPA will send addresses to the Central Geocoding Repository (CGR) and receive geocodes in return. The addresses and geocodes do not correlate with any individuals. Additionally, application specific data and various file types such as PDF, docx, xlsx, etc. are transmitted between RPA, the High Cost Verification Service (HCVS), Box, and Amazon S3.

[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.

USAC intentionally collects, via RPA, the name and state-issued engineering certification number for engineers verifying installation of broadband. Specifically, Blue Prism mailboxes send out process questionnaire forms to carriers, and these forms call for a engineer name and state-issued engineering certification number. Carriers upload the completed forms to Box, via the included link included in the original email. Blue Prism bots then transmit all submitted files in Box to USAC's X:drive. The Blue Prism bots then upload the carrier submitted questionnaires from USAC's X:drive to HCVS, via an API call, encrypted via AES 256 bit. Box, USAC's X:drive, and HCVS, are not components of RPA's authorization boundary. Blue Prism does not store the carrier submitted forms and therefore does not hold any PII.

RPA may incidentally collect PII. As part of the carrier services verification process, carriers submit evidence of service offerings to USAC's HCVS prior to Hyperscience ingesting them. Such evidence can include customer bills. Although carriers are instructed and expected to redact any/all customer information prior to submission, it is possible that carriers do not redact this information. In the case that the PII is not redacted, Hyperscience will collect this information upon digitization of the document.

C. 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")?

No.

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

Images of carrier submitted evidence, that may include incidental PII, are retained for a maximum of 60 days as defined by the Hyperscience retention policy configuration. Once the retention threshold is met, Hyperscience automatically deletes the images. PII intentionally collected via the process questionnaires (the engineer's name and certification number) is not stored within RPA.

1.5. Data Security and Privacy

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

Confidentiality	**__High**	**___Moderate**	**_X_Low**
Integrity	**__High**	**_X_Moderate**	**___Low**
Availability	**__High**	**___Moderate**	**_X_Low**

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

The system implementation is designed to be compliant with NIST SP 800-53 Revision 5 security and privacy controls, and will be assessed for compliance. The system operates on a FedRAMP authorized infrastructure, Amazon Web Services (AWS), provided by the General Support System (GSS) a USAC FISMA authorized system. Further, a System Security Plan (SSP) has been endorsed by system owner and authorizing official and RPA is under assessment for FISMA compliance, to be authorized prior to going live in production. This will address all pertinent controls for a Moderate system that protect data in a system. The data used by the system is provided internally and no external USAC clients or users will have access. The system will also inherit the Enterprise Common Controls (ECC) that incorporate security and privacy policy and procedure consistently across USAC systems.

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.

No.

1.6. Access to the Information

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

No RPA users have access to process questionnaires that include intentionally collected PII. Hyperscience production users can access carrier submitted evidentiary documentation which may include incidental PII. All users of RPA are USAC employees or USAC contractors.

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

Yes

USAC_FCC_PIA_RPA_-_Privacy_Edits_02.10_--_FINAL_CLEAN.docx

Final Audit Report 2023-02-14

Created:	2023-02-13
By:	Crystal Robinson (Crystal.Robinson@usac.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAzfk5Cd28L_q2ocU6l8KofVR-HrZpA2yp

"USAC_FCC_PIA_RPA_-_Privacy_Edits_02.10_--_FINAL_CLEAN.docx" History

Document digitally presigned by DocuSign\, Inc. (enterprisesupport@docusign.com)
2023-02-13 - 3:04:31 PM GMT

Document created by Crystal Robinson (Crystal.Robinson@usac.org)
2023-02-13 - 3:13:10 PM GMT

Document emailed to elliot.tarloff@fcc.gov for signature
2023-02-13 - 3:14:05 PM GMT

Email viewed by elliot.tarloff@fcc.gov
2023-02-13 - 6:58:43 PM GMT

Signer elliot.tarloff@fcc.gov entered name at signing as Elliot S. Tarloff
2023-02-14 - 8:20:39 PM GMT

Document e-signed by Elliot S. Tarloff (elliot.tarloff@fcc.gov)
Signature Date: 2023-02-14 - 8:20:41 PM GMT - Time Source: server

Agreement completed.
2023-02-14 - 8:20:41 PM GMT