GSA Equity Study on Remote Identity Proofing

Privacy Impact Assessment

September 5, 2023

POINT *of* CONTACT

gsa.privacyact@gsa.gov

GSA IT

1800 F Street NW

Washington, DC 20405

Stakeholders

Information System Security Manager (ISSM): Ryan Palmer
Program Manager/System Owner: Gerardo Cruz-Ortiz
Contracting Officer for Non-Federal Systems: Jeff Martin
Chief Privacy Officer: Richard Speidel

Signature Page

Signed:

DocuSigned by:
Ryan Palmer
6640A77DE3F842A...

Information System Security Manager (ISSM)

DocuSigned by:
Gerardo Cruz-Ortiz
827423346229451...

Program Manager/System Owner

DocuSigned by:
Jeffrey Martin
5A89AEDDFDF24E8...

Contract Specialist

DocuSigned by:
Richard Speidel
171D5411183F40A...

Chief Privacy Officer.
Under the direction of the Senior Agency Official for Privacy (SAOP), the Chief Privacy Officer is responsible for making sure the PIA contains complete privacy related information.

Document Revision History

Date	Description	Version of Template
01/01/2018	Initial Draft of PIA Update	1.0
04/23/2018	Added questions about third-party services and robotics process automation (RPA)	2.0
6/26/2018	New question added to Section 1 regarding Information Collection Requests	2.1
8/29/2018	Updated prompts for questions 1.3, 2.1 and 3.4.	2.2
11/5/2018	Removed Richard's email address	2.3
11/28/2018	Added stakeholders to streamline signature process and specified that completed PIAs should be sent to gsa.privacyact@gsa.gov	2.4
4/15/2019	Updated text to include collection, maintenance or dissemination of PII in accordance with e-Gov Act (44 U.S.C. § 208)	2.5
9/18/2019	Streamlined question set	3.0
2/20/2020	Removed email field from signature page	3.1

Table of Contents

SECTION 6.0 SECURITY

6.1 Who or what will have access to the data in the project? What is the authorization process for access to the project?

6.2 Has GSA completed a System Security and Privacy Plan (SSPP) for the information system(s) supporting the project?

6.3 How will the system be secured from a physical, technical, and managerial perspective?

6.4 Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII? If so, what are they?

SECTION 7.0 INDIVIDUAL PARTICIPATION

7.1 What opportunities do individuals have to consent or decline to provide information? Can they opt-in or opt-out? If there are no opportunities to consent, decline, opt in, or opt out, please explain.

7.2 What procedures allow individuals to access their information?

7.3 Can individuals amend information about themselves in the system? If so, how?

SECTION 8.0 AWARENESS AND TRAINING

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the project.

SECTION 9.0 ACCOUNTABILITY AND AUDITING

9.1 How does the system owner ensure that the information is being used only according to the stated practices in this PIA?

Document purpose

This document contains important details about the GSA Equity Study on Remote Identity Proofing. The GSA's Technology Transformation Services may, in the course of the Identity-Proofing Equity Study, collect personally identifiable information ("PII") about the people who use such products and services. PII is any information[1] that can be used to distinguish or trace an individual's identity like a name, address, or place and date of birth.

GSA uses Privacy Impact Assessments (PIAs) to explain how it collects, maintains, disseminates, uses, secures, and destroys information in ways that protect privacy. This PIA comprises sections that reflect GSA's privacy policy and program goals. The sections also align to the Fair Information Practice Principles (FIPPs), a set of eight precepts codified in the Privacy Act of 1974.[2]

A. System, Application, or Project Name:

The GSA Equity Study on Remote Identity Proofing

B. System, application, or project includes information about:

Members of the Public who volunteer as participants in the Identity-Proofing Equity Study.

C. For the categories listed above, how many records are there for each?

Up to 4000 workflow records.

---

[1] OMB Memorandum *Preparing for and Responding to the Breach of Personally Identifiable Information* (OMB M-17-12) defines PII as: "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." The memorandum notes that "because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad."

[2] Privacy Act of 1974, 5 U.S.C. § 552a, as amended.

D. System, application, or project includes these data elements:

GSA is partnering with multiple identity-proofing vendors to collect and analyze the needed data for the Equity Study. Table 1 below details which data is collected by the different identity-proofing vendors. Please note that Appendix A: PIAs for Non-Federal SubSystems covers specific details about each identity-proofing vendor. GSA will store all data collected by the identity-proofing vendors during the Equity Study on a GSA Google Drive for the duration of the study.

Table 1: Data collected by the various subsystems, vendors, and partners

Data Element	Source	Device Risk	Document Authentication	PII Validation	Recruitment	De-identified Dataset	Survey	Data Storage (GSA Google Drive)
Demographic Information (self-reported race, ethnicity, gender, age, income, education, and skin tone)	Participant					✓	✓	✓
Email Address	Participant				✓		✓	✓
Participant-Asserted Name	Participant			✓	✓			✓
Images of Identity Document (front/back)	Participant		✓	✓				✓
Machine Readable Zone from Identity Document (barcode) information	Vendor (Extracted from Identity Document Image)		✓	✓				✓
Identity Document Number	Vendor (Extracted from Identity Document Image)		✓	✓				✓
Identity Document Issue Date and Expiration Date	Vendor (Extracted from Identity Document Image)		✓	✓				✓
Face Reference (From Identity Document)	Vendor (Extracted from Identity Document Image)		✓			✓		✓

Data Element	Source	Device Risk	Document Authentication	PII Validation	Recruitment	De-identified Dataset	Survey	Data Storage (GSA Google Drive)
First, Middle, and Last Name from Identity Document	Vendor (Extracted from Identity Document Image)		✓	✓				✓
Date of Birth from Identity Document	Vendor (Extracted from Identity Document Image)		✓	✓				✓
Sex/Gender from Identity Document	Vendor (Extracted from Identity Document Image)		✓	✓				✓
Address from Identity Document (*Street, City, State, Zip Code)*	Vendor (Extracted from Identity Document Image)		✓	✓		✓		✓
Live image of participant's face (Selfie/headshot)	Participant		✓			✓		✓
Participant-Asserted Address (*Street, City, State, Zip Code)*	Participant			✓				✓
Participant-Asserted Social Security Number	Participant			✓				✓
Participant-Asserted Date of Birth	Participant			✓				✓

Data Element	Source	Device Risk	Document Authentication	PII Validation	Recruitment	De-identified Dataset	Survey	Data Storage (GSA Google Drive)
Participant-Asserted Phone Number	Participant			✓				✓
Phone Number matching the User identity	Vendor			✓				✓
Unique Mobile Device Identifiers	Vendor Participant (Collected by Vendor Client Side Code)	✓						✓
IP Address	Vendor	✓						✓
Device Geolocation (IP based)	Vendor	✓						✓
Device-behavioral Information (how the device and its applications are used)	Participant (Collected by Vendor Client Side Code)	✓						
Identity Proofing Results (True/False, type of check and errors)	Vendor	✓	✓	✓		✓		✓

Overview

The GSA "Equity Study on Remote Identity Proofing" will assess the impact of ethnicity, race, gender, income, and other demographic factors on the multiple components of identity proofing, which is the process of verifying that a person is who they say they are. GSA will test remote identity-proofing tools that include both biometric checks using facial verification technology as well as non-biometric methods like mobile-device account ownership and credit bureau records checks. NIST's SP 800-63-3 guidelines for remote one-to-one identity proofing serve as a framework for the study.

To conduct this study, GSA is partnering with identity-proofing vendors that are compatible with the study architecture and can meet agency Security and Privacy compliance requirements. Table 2 describes the service and vendors supporting the service.

Table 2: Vendor Services

System or Service	Provider
Recruitment	Rekrewt
Device Risk	Identity Proofing Vendors (See Appendix A)
Document Authentication	Identity Proofing Vendors (See Appendix A)
PII Validation	Identity Proofing Vendors (See Appendix A)
Results Analysis and Publication	Clarkson University, CITeR, Academic Journals
Survey	GSA Qualtrics
Data Storage	GSA Google Drive

Recruitment Service

GSA will be partnering with Rekrewt to enroll up to 4,000 participants residing in the US and US territories. Rekrewt will post advertisements on social media and assist GSA with building different outreach materials and networks. To track and provide compensation, GSA will share participants' names and email addresses with Rekrewt. To meet the study's demographic needs and tailor recruitment campaigns, GSA will send Rekrewt a regular status of the aggregated participant completion rate sorted by demographics. GSA recognizes that the "Equity Study on Remote Identity Proofing'' may not be accessible to all potential participants with disabilities because it requires volunteers to take photographs of their government-issued ID as well as a live "selfie" or headshot. GSA is also investigating other remote identity proofing solutions that are designed to be more accessible but still compliant with the guidelines in National Institutes of Standards and Technology (NIST) Special Publication (SP) 800-63.

Survey Administration

Qualtrics, which is licensed by GSA, will be used for all survey-type questions, including dissemination and acknowledgement of the study's Rules of Use, and Privacy Act Statement, collection of demographic information (race, ethnicity, gender, age, income, educational level), and capturing overall usability feedback. Survey responses are stored on Qualtrics for the purposes of managing quota requirements; this data is sent to the GSA Google Drive for long-term storage.

Qualtrics generates a unique ID that will be used for tracking completion status. Once participants' completion is determined, their name and email addresses are provided to Rekrewt.

Device Risk

While participants are using the study's web-based platform, GSA will collect information about the personal mobile device hardware and software as well as device-behavioral information for device risk detection; this information includes how the device and its applications are used to interact with the study's systems.

These device attributes are used to: 1) Uniquely identify a specific device so that it can be recognized upon return; and 2) Identify fraudulent intent based on a device's configuration (i.e., hiding behind an anonymous proxy). GSA may also store data in the browser's local storage as well as secure cookies to aid in re-identification.

An Mobile Network Operator (MNO) check is conducted to validate ownership of phone number, possession of device, and to confirm the address of record associated with the participant.

The final step in the workflow is an SMS security code phone check using a One-Time Password (OTP) that ensures that the same phone number entered during PII Validation is used.

Testing Vendors' Identity Proofing Document Authentication and PII Validation Products

Eligible participants who have consented to participation, will test multiple vendors' identity-proofing products that validate and verify the authenticity and possession of participants' identity documents while also validating the accuracy of their PII. See Appendix A for vendor software details.

The identity-proofing workflow collects the information specified in Table 1: Data collected by the various subsystems, vendors, and partners.

Identity-proofing vendors will collect, process, and transmit identity-proofing data and results to GSA. This information will then be deleted from vendors' systems within 24 hours of transmission; this is achieved by different mechanisms and ensured through a contractual requirement. Information collected through the Equity Study will be retained subject to GSA's System of Records Notice, as amended. GSA will retain records of this study in accordance with GSA's retention schedule for Customer Research and Reporting Records and any other applicable federal records schedules.

During Document Verification and Validation, GSA will present unbranded capture screens for the identity-proofing vendors. Each vendor will receive the information collected during the presentation of their designated screens, including a selfie capture. Vendors will decide if the provided documents are legitimate and determine whether the person pictured in the document matches the participant who just captured their own selfie. Vendor results are then transmitted to GSA and stored on the GSA Google Drive.

During PII Validation, GSA collects participants' PII and shares it with the applicable vendors to verify that the personal information provided by participants matches information available in general information databases.

Exit Survey

After the last step in the Equity Study, participants are redirected to a GSA-administered Qualtrics exit survey. The purpose of the exit survey is to gather usability feedback with the study. A copy of the exit survey results will be stored in the GSA Google Drive and Qualtrics.

Results Publication

Once the identity-proofing workflow is completed by all identity-proofing vendors and participants, GSA will remove all PII collected and create a report. GSA will share securely via (e.g., SFTP/Share file) the de-identified report with the academic partners, Clarkson University and the Center for Identification Technology Research (CITeR), that will analyze the results and assist GSA in publishing a peer-reviewed publication.

GSA will release the study's results in a peer-reviewed publication. The publication will present a statistical analysis of failures and successes for the proofing checks and explore the causes behind negative or inconclusive results. These results will help GSA understand the current technological barriers to equitable identity-proofing services for the public.

As stated above, this publication will assist GSA in making more informed decisions regarding identity verification capabilities. The outcome will also enable GSA to provide more equitable access to diverse populations that need to prove their identity.

SECTION 1.0 PURPOSE OF COLLECTION

GSA states its purpose and legal authority before collecting PI

GSA and the participating identity-proofing vendors are collecting the information to support the GSA Equity Study on Remote Identity Proofing. The study will test how one-to-one (1:1) remote identity-proofing methods like facial verification technology performs across various demographics to determine if vendor identity verification capabilities meet equity standards across the various demographics. This study will enable GSA to make a data driven decision on whether to pursue facial verification capabilities, to determine baseline performance metrics, and to provide real-world identity verification pass rate data to the broader Federal community.

The specific demographics and PII collected during this study are used to capture and verify the identity of an individual by comparing the government-issued ID with a live selfie and PII provided by the volunteers.

1.1 What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?

GSA is conducting the study pursuant to 6 USC § 1523 (b)(1)(A)-(E) and OMB Memo M-19-17.

1.2 Is the information searchable by a personal identifier, for example a name or Social Security Number? If so, what System of Records Notice(s) apply/applies to the information?

Yes, the information collected and retained by GSA can be retrieved by using a unique personal identifier. GSA's Login.gov SORN GSA/TTS-1 applies to the information involved in this study.

1.3 Has an Information Collection Request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)? If yes, provide the relevant names, OMB control numbers, and expiration dates.

Information Collection Title: GSA Equity Study on Remote Identity Proofing
Control Number: 3090-0328
Expiration Date: 2026-05-31

1.4 Has a records retention schedule been approved by the National Archives and Records Administration (NARA)? Explain how long and for what reason the information is retained.

Information collected through the Equity Study will be retained subject to GSA's System of Records Notice, as amended. GSA will retain records of this study in accordance with GSA's retention schedule for Customer Research and Reporting Records and any other applicable federal records schedules. The Customer Research and Reporting Records schedule requires that certain records related to research studies be destroyed 6 years after the end of the fiscal year in which the information was collected.

Identity-proofing vendors will collect, process, and transmit identity-proofing data and results to GSA. This information will then be deleted from vendors' systems within 24 hours of transmission. For more information on retention of each data element, please refer to Appendix A: PIAs for Non-Federal SubSystems.

SECTION 2.0 OPENNESS AND TRANSPARENCY

GSA is open and transparent. It notifies individuals of the PII it collects and how it protects, uses and shares it. It provides straightforward ways for individuals to learn about how GSA handles PII.

2.1 Will individuals be given notice before the collection, maintenance, use or dissemination of personal information about themselves? If not, please explain.

Yes. Before PII is collected, the participant will be required to review and agree to the study's Rules of Use (Appendix B) and Privacy Act Statement (Appendix C), which include consent to the collection of data. The T&Cs and Privacy Act Statement will also be available to participants and the general public via the equity study's landing page website and this PIA document. Additionally, there will be an information collection notice published on the Federal Register.

SECTION 3.0 DATA MINIMIZATION

GSA limits the collection of PII to what is needed to accomplish the stated purpose for its collection. GSA keeps PII only as long as needed to fulfill that purpose.

3.1 Why is the collection and use of the PII necessary to the system, application, or project?

The purpose of the Equity Study is to determine the impact of demographic factors (eg. race, ethnicity, gender, etc.) that impact the identity proofing process. To test identity-proofing methods and technology, GSA must collect PII data about the individual: identity document, name, date of birth, etc. PII must be collected to correctly validate and verify a participant's identity.

3.2 Will the system, application, or project create or aggregate new data about the individual? If so, how will this data be maintained and used?

Yes. The data collected by the identity-proofing vendors and shared with GSA will be sent on a transaction-by-transaction basis via API. All aggregation will be done by GSA in the GSA Google Drive. Aggregated de-identified data will be shared with CITeR researchers.

3.3 What protections exist to protect the consolidated data and prevent unauthorized access?

GSA requires all information systems that are publicly accessible to attain an "Authority to Operate" (ATO). The security measures described below are required to fulfill our ATO requirements.

Data:

- All data collected will be maintained within authorized GSA information systems as detailed by the relevant Systems of Records Notice, GSA/TTS-1 (Login.gov). The authorization process for these systems includes the testing of security controls, scanning of the system for vulnerabilities, and manual penetration testing.
- All data collected as part of the equity study is encrypted at all times.

User Accounts:

- Only GSA project staff that have passed background checks, and have a need to know will be provisioned access to the data.
- All user accounts with the ability to create, enable, modify, disable, and remove equity study information system accounts have role-based access controls implemented and are in compliance with GSA security requirements.
- Notifications are generated to account managers in the following conditions:
    - Accounts are no longer required
    - Users are terminated or transferred; and
    - Individual information system usage or need-to-know changes

- All user accounts undergo an annual review to ensure compliance with account management requirements.

3.4 Will the system monitor the public, GSA employees, or contractors?

No. GSA and identity-proofing vendors will not be monitoring participants. The Equity Study is limited to testing vendors' identify proofing products using volunteer participants.

3.5 What kinds of report(s) can be produced on individuals?

GSA compiles a de-identified report and shares it with CITeR and Clarkson University for a statistical analysis of the results. Furthermore, GSA may consider vendor requests to share their portion of the results from the de-identified report.

From the data stored on the GSA Google Drive, GSA can compile analytical reports, although no other reports are identified at this time (see Table 1 for details).

3.6 Will the data included in any report(s) be de-identified? If so, what process(es) will be used to aggregate or de-identify the data?

GSA will analyze fields to understand whether a participant passed each stage, what error codes mean, etc. This de-identified information will be passed to CITeR researchers for the final publication.

The final peer-reviewed publication will be de-identified and all data will be presented in graphs and in groupings. The publication will only contain demographic information and de-identified study results (Refer to Table 1 for details.) The following processes will be leveraged to de-identify data:

- Participant information is masked,
- Participant names, date of birth, social security numbers, addresses, and phone numbers are suppressed,
- No direct identifiers will be included

SECTION 4.0 LIMITS ON USING AND SHARING INFORMATION

GSA publishes a notice about how it plans to use and share any PII it collects. GSA only shares PII in ways that are compatible with the notice or as stated in the Privacy Act.

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. The Equity Study is a discrete study to evaluate the effectiveness and to test performance, fairness, and equity of several third-party vendors' remote identity proofing software. The data is strictly used for the Equity Study purposes. Table 3 provides additional details.

Table 3: PII Elements

Data Collected	Data Use	System or Service
Demographic Information (self-reported race, ethnicity, gender, age, income, education, and skin tone)	Used to look for trends in identity proofing results.	Survey, Results Analysis
Email Address	Used to share compensation details at the end of study and needed by the survey platform. If participants agree, GSA may also contact them via email for future studies.	Survey, Recruitment, PII Validation
Participant Name	Used to share compensation details at end of study	Survey, Recruitment, PII Validation
Images of Identity Document (front/back)	Used for the "document authentication" identity-proofing step and check that the identity document is legitimate.	Document Authentication, Results Analysis
Identity Document Machine Readable Zone information (barcode)	Used to verify that the identity document is legitimate.	Document Authentication
Identity Document Number	Used to verify that the identity document is legitimate.	Document Authentication
Identity Document Issue Date and Expiration Date	Used to verify that the identity document is valid.	Document Authentication
Face reference (picture from Identity Document)	Used to verify that the identity document is legitimate, as well as the "biometric comparison" identity proofing step to compare the participant's Face reference to their selfie.	Document Authentication, Results Analysis

Data Collected	Data Use	System or Service
First, Middle, and Last Name (from Document)	Used to verify the participants' identity matches the identity document.	Document Authentication, PII Validation
Date of Birth (from Document)	Used to verify the participants' identity matches the identity document.	Document Authentication, PII Validation
Sex/Gender (from document)	Used to verify the participants' identity matches the identity document.	Document Authentication, PII Validation
Address Street, City, State, Zip Code (from Document)	Used to verify the participants' identity matches the identity document.	Document Authentication, PII Validation
Live image of your face (or "Selfie")	Used to verify that the Identification document belongs to the participant.	Document Authentication
Participant-Asserted Address: Street, City, State, Zip Code	Used to verify that the participant is who they claim they are.	PII Validation
Participant-Asserted Social Security Number	Used to verify that the participant is who they claim they are.	PII Validation
Participant-Asserted Date of Birth	Used to verify that the participant is who they claim they are.	PII Validation
Participant-Asserted Phone Number	Used to verify that the participant is who they claim they are.	PII Validation, Device Risk
Phone Number matching the User identity	Used to verify that the participant is who they claim they are.	Device Risk
Unique Mobile Device Identifiers	Used to compute a risk assessment of the mobile device used by the participant to access the study.	Device Risk
IP Address	Used to compute a risk assessment of the mobile device used by the participant to access the study.	Device Risk
Device Geolocation (IP based)	Used to compute a risk assessment of the mobile device used by the participant to access the study.	Device Risk
Device-behavioral Information (how the device and its applications are used)	Used to compute a risk assessment of the mobile device used by the participant to access the study.	Device Risk

Data Collected	Data Use	System or Service
Identity Proofing Results	Used for determine demographic bias in data	Device Risk, PII Validation, Document Authentication

4.2 Will GSA share any of the information with other individuals, federal and/or state agencies, or private-sector organizations? If so, how will GSA share the information?

GSA is limiting access to the data collected during the Equity Study to the TTS Team and contractors supporting the Equity Study.

GSA will provide the Recruitment partner email address and participant name for compensation purposes via Google products.

Identity Proofing Vendors will collect data during workflow and share results with GSA, and GSA will prohibit further access to data upon receipt of data.

GSA will share securely via (e.g., SFTP/Share file) a de-identified report with the academic partners, Clarkson University and CITeR; CITeR and Clarkson will analyze the results and assist GSA in writing a peer-reviewed publication.

4.3 Is the information collected directly from the individual or is it taken from another source? If so, what is the other source(s)?

Study participants provide PII directly to both GSA and Identity Proofing vendors. Identity-proofing vendors cross-reference participant-provided PII with their respective repositories. The source of the data collected in each identity-proofing vendor's external repositories is described in their privacy policies.

GSA will not have access to any information in the identity-proofing vendors' repositories, e.g., financial credit reports.

4.4 Will the system, application, or project interact with other systems, applications, or projects, either within or outside of GSA? If so, who and how? Is a formal agreement(s) in place?

Internal Systems

The Equity Study project is composed of the following applications within GSA:

- Qualtrics
- Identity Verification API (IDVA)
- GSA-Google Drive

Qualtrics, which is licensed by GSA, will be used for all survey-type questions, including dissemination and acknowledgement of the study's Rules of Use, and consent language, collection of demographic information (race, ethnicity, gender, age, income, educational level), and capturing overall usability feedback. Survey responses are stored on Qualtrics for the purposes of managing quota requirements; this data is also sent to the GSA Google Drive for long-term storage.

The Identity Verification API (IDVA) is the technology backbone of the Equity Study. IDVA serves as an "orchestration layer" to deliver a consistent user interface to participants and connect the Identity Proofing vendors' services. IDVA is an internal GSA system; only the Equity Study Team can access IDVA as defined by GSA requirements. GSA reviews accounts annually for compliance with account management requirements. See SECTION 6.0 SECURITY for more information.

The GSA Google Drive is the long-term storage location for the data collected in both Qualtrics and IDVA. Only the Equity Study Team can access the Google Drive. For details see 6.1 Who or what will have access to the data in the system, application, or project? What is the authorization process to gain access?

External Entities

The Equity Study will also interact with the following systems and organizations external to GSA:

- Rekrewt
- Identity Proofing Vendors (See Appendix A)
- CITeR and Clarkson University

Rekrewt is under contract to post advertisements on social media and assist GSA with building different outreach materials and networks. To track and provide compensation, GSA will share participants' names and email addresses with Rekrewt. To meet the study's demographic needs and tailor recruitment campaigns, GSA will also share with Rekrewt a regular status of the aggregated participant completion rate sorted by demographics.

GSA has contracted with multiple Identity-Proofing vendors to collect PII and perform identity-proofing checks electronically. This data is transmitted to GSA through IDVA on a transaction by transaction basis. GSA will describe the vendors' use and retention of data in a Privacy Act Statement presented to participants. GSA will also provide a link to the identity-proofing vendors' Privacy Policies in the study's consent language. The privacy policies describe the vendors' commercial services in general, and as a result may contain information about services that are not applicable to this study. However, vendors will retain and use participant data only in accordance with GSA's written agreements with each vendor as described in the Privacy Act Statement.

All identity-proofing vendors' systems have undergone a Security and Privacy Review; each vendor has a contractual agreement with GSA defining applicable privacy and security controls. Furthermore, each vendor has submitted a Non-Federal Privacy Impact Assessment (PIA). For details on identity-proofing vendor systems' access controls, see Non-Federal SECTION 5.0 SECURITY in Appendix A.

Researchers from CITeR and Clarkson University will receive a bulk de-identified data set of proofing results and demographic information (See Table 1). They will analyze results and assist GSA in submitting them to a peer-reviewed publication.

SECTION 5.0 DATA QUALITY AND INTEGRITY

GSA makes reasonable efforts to ensure that all PII it maintains is accurate, relevant, timely, and complete.

5.1 How will the information collected be verified for accuracy and completeness?

Accuracy

For purposes of the study, accuracy is measured by two components:

- false positives: accepting people who are pretending to be someone else or who have invalid identification documents, and
- false negative: rejecting people who present valid identity documents.

The primary purpose of the study is detecting false negatives. The study relies on participants providing accurate information and participating in good faith. The identity-proofing vendors will determine whether the participants are presenting valid information and will provide detailed error codes when the proofing systems determine that a participant is presenting

invalid information. GSA also relies on the accuracy of the data included in each identity proofing vendors' systems for validation and verification.

To test the Identity Proofing vendors' capability to minimize false positives, the Equity Study will employ a spoof testing vendor to conduct spoofing testing (e.g., using an invalid/counterfeit or forged identity document; a person whose selfie does not match identity document) concurrently with participant submissions to ensure that the vendors' capabilities are accurately validating and verifying a user's submitted information.

The Equity Study team will work with the academic partners to include proofing failure reasons in the analysis. Inaccuracies that result in identity proofing failures will not be used for purposes other than research; therefore, any inaccuracies in the collected data will not adversely affect participants.

Completeness

Participants must provide all requested information in order to complete the study. GSA will not include incomplete participant data in any report or data storage system.

SECTION 6.0 SECURITY

GSA protects PII from loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

6.1 Who or what will have access to the data in the system, application, or project? What is the authorization process to gain access?

Access to the information collected under this Equity Study is on a need-to-know basis and only for business, legal, or regulatory related requests. Table 1 shows a breakdown of the information collected and accessible by different organizations and systems.

- **Identity-proofing vendors' staff:** will have access to the information for the duration of each transaction. This information will then be deleted from vendors' systems within 24 hours of transmission of identity-proofing data and results to GSA
- **GSA Equity Study Team** will have access to all study data stored on GSA information systems. GSA Staff and Contractors have completed GSA background checks required to handle PII data. No PII may be removed from GSA information systems. If additional access is requested, the Equity Study project manager in consultation with the GSA

Information Systems Security Officer (ISSO) will approve access. Additional details have been documented in the System Security and Privacy Plan (SSPP).

- **CITeR and Clarkson researchers:** Will receive a file containing de-identified identity-proofing results and demographic information.
- **Rekrewt:** Will receive a file containing the name and email addresses of participants who completed the study.

6.2 Has GSA completed a System Security and Privacy Plan (SSPP) for the information system(s) or application?

IDVA developed a system security plan and performed an assessment according to the GSA Lightweight Authority to Operation process.

Authority to Operate (ATO) was granted on *December 21, 2021.*

6.3 How will the system or application be secured from a physical, technical, and managerial perspective?

IDVA, GSA-Google drive, and all the equity study platforms comply with the requirements in National Institutes of Standards and Technology (NIST) Special Publication (SP) 800-53 and GSA's Security processes as outlined by CIO-IT Security-14-68 and CUI policies. GSA implements multi factor authentication for all access to the platform and data to prevent unauthorized access. All PII data is encrypted data in transit via TLS 1.2+ and and at rest via AES-256 to ensure data is not exposed.

GSA implements managerial control and review processes to ensure that these protections are in place. GSA conducts assessments of information systems prior to their authorization to operate. GSA monitors the status of the information system by scanning the system for vulnerabilities. Additionally, GSA conducts security impact analysis when changes are made to the system to ensure security controls are not impacted.

All vendor services and platforms comply with GSA security requirements as documented in Non-Federal SECTION 5.0 in Appendix A.

6.4 Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII? If so, what are they?

Yes, IDVA has an incident response plan that employs automated mechanisms to integrate audit review, analysis, and reporting processes. IDVA's monitoring system automatically reports suspicious activity; the IDVA team will review and analyze these notifications to determine their validity and appropriate action if any.

Additionally, IDVA uses tools from the cloud service provider that heuristically detect both security incidents and potential breaches of PII. These tools both offer additional insight on avenues of breach that may not be alarmed directly, and provide real-time insight about trends and flows of data to further enhance responsiveness. These notifications are sent to idva@gsa.gov and are acted upon as defined in the IDVA Operations and Maintenance checklist. In the event of a breach or suspected breach, IDVA will coordinate incident response with the GSA enterprise incident response team.

All identity-proofing vendors have internal incident response teams that are responsible for establishing all incident response and escalation procedures to ensure timely and effective handling of all situations. Identity-proofing vendors shall report incidents to GSA by following processes established in the relevant contracts and agreements. All identity-proofing vendors must also provide penetration testing results and vulnerability scans to GSA before being integrated into the Equity Study's production environment.

SECTION 7.0 INDIVIDUAL PARTICIPATION

GSA provides individuals the ability to access their PII and to correct or amend it if it is inaccurate. If GSA exempts a system or program from access, amendment and other provisions of the Privacy Act, it notifies the public of that exemption.

7.1 What opportunities do individuals have to consent or decline to provide information? Can they opt-in or opt-out? If there are no opportunities to consent, decline, opt in, or opt out, please explain.

Participation in the Equity Study is voluntary. If a participant does not consent to the Equity Study, they may not participate and no information beyond what was collected during recruitment will be collected. Once information is submitted participants may no longer opt-out of participation. If a participant declines, opts out, or they are not eligible to participate, GSA will delete all identifying data associated with that participant. GSA may retain non-identifying data (e.g. demographic information) to study drop-off rates.

7.2 What procedures allow individuals to access their information?

Participants have the opportunity to review/update information during the flow. After submission, participants do not have an in-flow method to access the submitted information.

However, participants may submit a Privacy Act request (see Appendix C: Privacy Act Statement) to obtain all relevant records of their participation.

Individuals seeking access to their records in this system of records may submit a request by following the instructions provided in 41 CFR part 105-64.2.

7.3 Can individuals amend information about themselves? If so, how?

Participants will have the ability to modify their information as part of their submission. Components of the workflow will allow for review and multiple resubmissions, but once submitted, data will not be modifiable.

Individuals have the opportunity to correct their Social Security Number, Phone Number, and Mailing Address before submission. Once an individual completes the identity proofing flow they will not have the opportunity to edit their information. System administrators and other privileged users do not have access to modify PII on a user's behalf.

Participant information is deleted from vendors' systems within 24 hours of transmission of identity-proofing data and results to GSA. Therefore, participants will not have the opportunity to amend the information submitted to the third parties after submission. Some identity-proofing vendors may have processes to amend information according to their entries in Section 6.3 in Appendix A.

SECTION 8.0 AWARENESS AND TRAINING

GSA trains its personnel to handle and protect PII properly.

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the system, application, or project.

All GSA staff and contractors are trained on how to identify and safeguard PII. In addition, each employee must complete annual privacy and security training. Those who need to access, use, or share PII as part of their regular responsibilities complete additional role-based training. Staff

who fail to complete these trainings may be subject to disciplinary action and may eventually lose system access.

Identity-proofing vendors provide their own privacy and security training to employees as required by contractual agreements and described in Appendix A, SECTION 7.0 AWARENESS AND TRAINING

CITeR researchers (related to human subjects) take the Collaborative Institutional Training Initiative (CITI) Training-Biomedical Research course, which outlines major topic areas and concepts that are specific to types of research, roles in the protection of human subjects, and advanced modules on informed consent topics, vulnerable populations, stem cell research, phase I research, data and safety monitoring, big data research, mobile apps research, and disaster and conflict research. It offers historic and current information on regulatory and ethical issues important to the conduct of research involving human subjects. This course also reflects the 2018 Requirements of the Common Rule.

Rekrewt personnel personnel provide their own privacy and security training to employees as required by their contractual agreements. All staff members complete "HHS/NIH Contractor Information Security Awareness, Privacy, and Records Management" training on an annual basis.

SECTION 9.0 ACCOUNTABILITY AND AUDITING

GSA's Privacy Program is designed to make the agency accountable for complying with the Fair Information Practice Principles. GSA regularly checks that it is meeting the requirements and takes appropriate action if it is not.

9.1 How does the system owner ensure that the information is used only according to the stated practices in this PIA?

Vendor safeguards and privileged access controls are documented in the SSPP. Contracts with the identity-proofing vendors also include provisions requiring the vendors only use the data as described in the accompanying contract. Specifically, the identity-proofing identity-proofing vendors' contracts require that they submit a written attestation of data deletion at the end of the study.

GSA reviews the security and compliance status of any third-party systems that data is shared from throughout the duration of the study. Ensuring that these systems maintain functioning security and privacy controls.

GSA has incorporated privacy controls throughout the design and development of the Equity Study. All design and identity-proofing vendor changes are reviewed for privacy impacts.

Appendix A: PIAs for Non-Federal SubSystems

Non-Federal System Overview:

GSA is partnering with multiple identity-proofing vendors to collect and analyze the needed data for the Equity Study. This Appendix covers specific details about each identity-proofing vendor.

Non-Federal Section A. System, Application, or Project Name:

TransUnion

TransUnion TruValidate Document Verification via AuthenticID DaVinci Connector (Government photo ID capture, verification and validation)

Socure

Socure's ID+ platform is a Software as a Service (SaaS) product that will integrate with the Identity Verification API (IDVA) to verify the identity of individuals participating in an identity equity study.

Jumio

Jumio ID and Identity Verification

LexisNexis

The existing NonFederal Privacy Impact Assessment for LexisNexis found in https://www.gsa.gov/reference/gsa-privacy-program/privacy-policy-for-nonfederal-systems also applies to the Identity Proofing Equity Study. Please refer to that document for LexisNexis' answers to the questions in this appendix.

Incode

Incode Omni

red violet

IDICore™ and coreIdentity™ Platforms

Non-Federal Section B. GSA Client:

GSA TTS - Identity Portfolio

Non-Federal Section C. System, application, or project includes information about:

Members of the general public who volunteer for the study.

Non-Federal Section D. System, application, or project includes these data elements

TransUnion

TU services will provide a web-based application interface for use in real time identity verification processes. In the case of Government photo ID checking, the experience is hosted on behalf of GSA. The following elements will be included in this process:

Controlled Unclassified Information:

1. Participants' Full Name,
2. Date of Birth,
3. Physical Address,
4. Images of drivers license and selfie captured by the user's device,
5. the data printed or encoded (barcode) on the Government Identification card (e.g. driver's license),
6. Biological characteristics derived from a picture of the participant face (a "selfie"), and
7. Biological characteristics derived from a photo of participant identity document, which also contains a photo of participant.

Overview of User-Provided Data Persistence:

CUI will be provided by users via IDVA to be evaluated by TransUnion services. The TransUnion solution for IDVA will destroy these data inputs (see Controlled Unclassified Information earlier in this section) as described below:

1. Images of driver's license and selfie image) – destroyed within 24 hours of transaction start.
2. All other CUI – This data is not persisted (i.e. not written to logs, databases or any other TransUnion system), rather it is evaluated in system memory only until the response is forwarded to IDVA.

Socure

Socure may collect and use:

- Identifiers: First and last name, email address, current and past addresses, phone number, and date of birth.
- Geographic data: Address, including city, state, country of residence, and postal code; IP address; and device geolocation.
- Device information: The user's computer or mobile device operating system type and version, model and manufacturer, browser type, screen resolution, RAM and disk size, CPU usage, device type (e.g., phone, tablet), IP address, unique identifiers , language settings, mobile device carrier, radio/network information (e.g., Wi-Fi, LTE, 3G); device behavioral information (how the device and its applications are used such as accessibility data); and other data (i.e. CPU data) used in misbehavior detection.
- Government-issued identity documents: Identifiers, including name, address; date of birth; national, state or local identification number (e.g. passport, driver's license or state ID number), and more – depending upon the design of each jurisdiction's document. Also, barcodes and machine-readable zone (MRZ) data, and headshot photographs contained in the document.
- Face images and data: Headshots from government-issued identity documents; selfie photographs. These images will be processed to derive metadata and biometric information, such as data about the applicant's face geometry.

Jumio

GSA will integrate Jumio services enabling Jumio to process the following information from GSA End-Users via a web or mobile interface:

- Scan of GSA Approved Identification Documents (e.g., Passport, Driver's License, Visa, etc.);
- Data extracted from the Scan of GSA Approved Identification Documents (e.g., photo, name, identity document number, age, sex, etc.);
- Images collected via a recording in a web or mobile interface at time of transaction (i.e., a "Selfie"); and
- Biometric Data

Incode

Incode will provide the remote identity proofing workflow, which includes **Document Authentication, Passive Liveness, and Facial Recognition.** GSA can configure the workflow to meet its business needs.

Document Authentication asks the user to upload a photo of the front and back of their government-issued credential (ID, passport, etc.). Over 25 checks run within seconds to verify the credential's validity, and optical character recognition (OCR) extracts the data. The photo on the credential is translated into a binary template , or a mathematical representation of the face that cannot be reverse engineered. With Document Authentication, data elements include:

- The user's biographic data from the credential (e.g., first name, last name, address, date of birth, license number)
- The user's credential photo
- The barcode on the back of the credential

Passive Liveness asks the user to take a selfie (a photo of their face). Incode's passive liveness technology ensures the person is a real, live person with no user effort (e.g., no need for the user to blink or move). The selfie photo is also translated into a binary template. With Passive Liveness, the data element is the user's selfie photo.

Facial Recognition compares the binary template of the credential photo to the binary template of the user's selfie to confirm a match/no match result With Facial Recognition, the data elements are the binary templates. Binary templates are strings of code representing facial characteristics that cannot be reverse engineered.

red violet

Red violet's KYC APIs search against names & aliases, date of birth, age, address, phone number, and social security number.

In addition, red violet can search against the following using our idiCore platform:

- Social Security number,
- IP Address,
- Estimated Income,
- Assets,
- Relatives & Associates,
- Deceased Indicator,
- Employment History

For the GSA equity study deployment, red violet will process the data sent by GSA for an Identity Verification check; once the process is completed, the data will be discarded after the verification process is complete.

Non-Federal Section E. The purpose of the system, application, or project is:

TransUnion

For the purpose of identity verification using a government identity document, the system will collect images of the identification card for the purpose of conducting automated anti-fraud routines designed to consider and report on the risk associated with the document as presented (e.g. false document), optical character recognition will convert the image of Full Name, Date of Birth and Physical address to text. Images, PII and transaction meta-data are destroyed within 24-hours as required by GSA. Submitted data which will be shared with GSA for its use.

Socure

IDVA will integrate with Socure's identity verification services in order to effectively and quickly verify that an online interaction is a genuine person and that they are who they say they are. The nature of the modern internet is that it is common for fraudsters to impersonate good people using stolen personal information. Hence, the agency offering online services must verify that each new online interaction is truly the genuine person who is entitled to open or access that account. Socure only collects the minimum necessary information in order to perform high-accuracy, automated checks on the identity information in order to let good people proceed while blocking suspicious and fraudulent entities.

Jumio

In order to verify the authenticity of government-issued photo identification documents and the identity of GSA End-Users, Jumio Corporation, a United States Corporation with headquarters in Palo Alto, California, is providing identification document ("ID") and identity verification services to GSA.

The GSA will use Jumio services to process information collected from GSA End-Users via a web or mobile interface hosted by GSA. The information is transmitted securely using the encryption methods described in Section 5. Jumio reviews the ID and verifies the authenticity of the document (i.e., ID verification). Jumio's biometric technology enables Jumio to verify that the ID belongs to the GSA End-User making the transaction (i.e., identity verification). Jumio compares the GSA End-User's facial biometrics from a selfie to the photo on the ID document, and generates a check for facial similarity. The similarity check, which is powered by informed Artificial Intelligence (AI), indicates the confidence level that the image in the selfie matches the photo in the identity document.

Results of Jumio's review of the transaction (e.g., verified, rejected) are communicated to GSA using a secure communication channel. GSA uses the information provided to make an independent assessment and makes the final decision whether to proceed with the GSA End-User relationship. GSA also provides the GSA End- User with the opportunity for assistance through a video verification agent (e.g., technical assistance). The video verification agent engages the GSA End-User in a live video to collect the image of the ID and an image of the GSA End-User. The information is transmitted to Jumio for verification.

GSA receives access to the captured images, extracted data, and results of the transaction. GSA controls the deletion of the information collected for the transaction at the conclusion of the transaction via the integration with Jumio. Jumio does not further retain PII, including any biometric data used for identity verification, in accordance with the retention set by GSA within the Jumio portal.

Incode

Incode's identity proofing workflow includes validating the credential for authenticity and extracting the data. PII elements typically captured in this process include first name, last name, date of birth, address, driver's license number, the facial photo on the credential, and the contents of the barcode on the back of the credential. The identity proofing workflow also captures a selfie (an image of the user's face). The selfie image and the facial photo on the credential are both converted to binary templates (strings of code representing the face that cannot be reverse engineered.) GSA can configure the workflow to decide which type of PII is collected and from who.

Incode will not store data and therefore, inherently lacks the ability to share, sell, market, or otherwise use participant information, including for enrichment purposes. GSA owns and controls the data, deciding which data to store or delete. Incode will follow the Zero Data Retention Policy set by GSA and delete data within the timeframe determined by GSA.

Incode uses only government-validated sources of truth for increased privacy and accuracy. All data processed by the system is classified as confidential and encrypted both in transit (HTTPS with TLS 1.2 and TLS 1.3) and at rest (AES with 256-bit keys). Incode follows industry best practices and is compliant with key data standards, including SOC 2 Type II.

red violet

IDI's coreIDENTITY platform is a comprehensive suite of identity solutions that encompasses the full customer identity lifecycle from acquisition to onboarding and beyond with out-of-the-box APIs and customizable workflows. IDI's KYC APIs are part of the coreIDENTITY suite of products. The KYC APIs provide a full range of capabilities for identity data verification and augmentation.

The APIs are easily integrated into identity workflows such as onboarding, pre-fill, contact information cleanup, amongst others. The APIs are unique as they have a full range of identity match information such as exact/partial/no match results, match and risk scores, and reason codes. Included in the APIs are synthetic ID fraud signals and death event indicators.The KYC APIs allow enterprises to implement low friction identity verification and augmentation workflows while meeting compliance and privacy needs.

The IDICoreTM and coreIdentityTM Platforms are designed to comply with applicable laws, to include the Gramm-Leach-Bliley Act and Driver's Privacy Protection Act. PII within the system is collected from public records and proprietary data sources, who attest that they have the legal right to license the data for these purposes . Data is collected in either a batch format via APIs depending on agreements and the data source provider. Red violet employs rigorous credentialing and auditing processes to vet its business customers and help ensure that they only use PII derived from the system for lawful business purposes. Red violet also employs information security best practices to safeguard the information contained within the system. For example, Red violet is SOC 2, Type 2 compliant, PCI Level 1 compliant, and the system aligns with ISO 27001 and other industry best practices. PII-claims data will only be used for the verification process and be discarded after the verification is complete.

Non-Federal SECTION 1.0 OPENNESS AND TRANSPARENCY

1.1 Are individuals given notice before the collection, maintenance, use or dissemination of personal information about themselves? If not, please explain.

Yes. Refer to the Equity Study PIA Section 2.1 “Will individuals be given notice prior to the collection and/or sharing of personal information about themselves? If not, please explain.” for details.

Non-Federal SECTION 2.0 DATA MINIMIZATION

2.1 Why is the collection and use of PII necessary to the system, application, or project?

Refer to the Equity Study PIA Section 3.1 “Why is the collection and use of the PII necessary to the system, application or project?” for details.

TransUnion

TransUnion services will be responsible for supporting IDVA to validate the identity of web-based users for the purpose of evaluating the equitable performance of identity-proofing technologies. Collection of PII is necessary to verify users' identities in a manner that meets GSA's requirements for this study.

Socure

The purpose of the GSA Equity Study is to ensure that GSA considers the consequences of its choice of an identity verification vendor on different demographics, especially protected classes. Collection of PII for verification is, by definition, inherent in the identity verification process. Identity verification is a necessary gateway to allow individuals to access government services and websites while blocking fraudsters using misappropriated personal information. Socure only collects PII that is useful for identity verification and fraud prevention, for which there is sound and plentiful evidence for its usefulness in online identity verification. This is limited to name, address, phone, email, national identifier, date of birth, device information, and the identity document and selfie.

Jumio

Jumio collects, uses, and discloses individual users' information only as directed by GSA. GSA has ensured that only the minimum amount of PII is collected to provide the service and that GSA deletes the information collected for transactions at the conclusion of the transactions.

Incode

Incode will collect PII in order to perform document verification. Upon completion of the remote identity proofing session, the PII collected will be transmitted to GSA's system and deleted from the Incode Omni platform so that Incode is following GSA's Zero Data Retention Policy requirements.

red violet

No additional response provided.

2.2 Will the system monitor the public, GSA employees, or contractors?

No. Refer to the Equity Study PIA Section 3.4 "Will the system monitor the public, GSA employees or contractors?" for details.

2.3 What kinds of report(s) can be produced on individuals?

Refer to the Equity Study PIA Section 3.5 "What kinds of report(s) can be produced on individuals?" for details.

TransUnion

This system does not incorporate any individual monitoring capability of any kind. All PII, images and metadata are purged immediately of the transaction, the system will be able to report the following to GSA:

- Images of the government ID
- Image of the participant selfie
- Data scanned from the government ID (e.g. PII, barcode)
- System information (e.g. metadata such as transaction ID, date, time, document disposition such as accept or reject)

Socure

Socure's ID+ does not have the functionality to produce reports on individuals. Aside from the API response, there is no statement describing individuals. Socure's service is an automated API (application programming interface) that GSA will call. Socure's customer dashboard allows GSA employees to view information on a per-transaction basis, but it does not permit export of PII.

Jumio

Jumio provides GSA with the information collected from the Equity Study participant and a transaction result.

GSA instructs Jumio to delete all information, including any biometric data, collected in accordance with the services immediately after the conclusion of the transaction. Jumio does not further retain any PII past the transaction and no other reports can be generated from Jumio using GSA End-User PII.

Incode

Incode will follow GSA's Zero Data Retention Policy and delete all data once transferred to GSA, and as such Incode inherently will not have data to generate reports on individuals.

red violet

As red violet does not store any query data, we will not have the capability to monitor any subsequent transactions and/or enrollment requests that the user submits. Red violet can provide reports in aggregate views but these views will not be able to be traced to individual requests. For example, Red Violet will be able to provide a view of the total number of verifications the system has performed; however, it will not be able to provide information

contained in the query for the transaction, that information is discarded after the verification process is complete.

2.4 Will the data included in any report(s) be de-identified? If so, what process(es) will be used to aggregate or de-identify the data?

Refer to the Equity Study PIA Section 3.6 "Will the data included in any report(s) be de-identified? If so, what process(es) will be used to aggregate or de-identify the data?" for details.

TransUnion

User transaction data will be deleted within 24 hours of the user validation transaction within all vendor systems and logs, therefore all activity will become de-identified. Reporting is only possible based upon:

- Billing ID (which cannot be mapped to user data at the completion of the transaction).

Socure

Socure will not be producing the Equity Study report; GSA will produce it. Socure can limit the identifiability of information that it returns to GSA by use of a non-PII record locator for each individual's transaction. Socure can otherwise work with GSA to limit the transmission of PII through de-identification (to the extent possible) or other privacy enhancing techniques.

Jumio

Jumio maintains de-identified data about the details of the transaction to provide aggregated analytics reports. For example, Jumio may report on the number of transactions, methods of collection, and results of verification (i.e., passed, failed), among others. The de-identified and aggregated data used is not tied to any PII listed in Section D.

Incode

Incode will follow GSA's Zero Data Retention Policy and delete all data once transferred to GSA, and as such Incode inherently will not have data to generate reports that contain PII.

red violet

No additional response provided.

Non-Federal SECTION 3.0 LIMITS ON USING AND SHARING INFORMATION

3.1 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. Refer to the Equity Study PIA Section 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?" for details.

TransUnion

Information that is collected only includes data or metadata associated with the identity verification process and determined as necessary by GSA for the purposes of its Equity Study. PII is collected only for specific and explicitly authorized purposes. The PII data elements to be collected are only those elements required for the study and are not used for any other purposes as described in D. System, application, or project includes these data elements above.

GSA requires its vendors to purge data within 24 hours of transmission.

Socure

Socure only collects PII that is useful for identity verification and fraud prevention, for which there is sound and plentiful evidence for its usefulness in online identity verification. This is limited to name, address, phone, email, national identifier, date of birth, device information, and the identity document and selfie.

Jumio

Jumio and GSA collaborated to review the information and limit the collection to only the information necessary to carry out the ID and identity verification services.

The information in the project is limited to only what is needed to carry out the ID and identity verification by Jumio.

Incode

Incode will collect and process only the minimum PII data elements that GSA has a legitimized basis for using. As described in Section D, PII elements typically captured in the identity proofing process include first name, last name, date of birth, address, driver's license number, the facial photo on the credential, the contents of the barcode on the back of the credential, and a selfie (an image of the face). These PII elements ensure an accurate and secure identity verification, confirming that the credential is valid and unaltered and that the person presenting the credential is the true owner of the identity. The PII elements collected, and the

entire identity proofing workflow, are configurable by GSA. GSA will determine which PII is collected and from whom.

Incode will adhere to GSA's Zero Data Retention Policy. As Incode will not store any data, Incode inherently lacks the ability to sell, market, share, or otherwise use participant information, including for enrichment purposes.

red violet

Red violet will collect PII claims made by the user such as Names & Aliases, Date of Birth, Age, Address, Phone Number, Social Security number. The user's PII claims will be verified by Red violet as part of the equity study. The information from the PII claims will not be used for any other purpose. In addition, the information will only be used for the verification process and be discarded after the verification is complete. As such, red violet will adhere to the GSA's Zero Data Policy, deleting all transactions after they are complete.

As part of its Privacy Policy, red violet partners with its executive management personnel, legal personnel, compliance personnel, and other qualified personnel to determine which information to make available via the system, for which purposes, and to which types of potential customers. Red violet only makes information available via its system where such information is: (i) permitted by applicable laws to be used for the purpose and (ii) the benefit of providing the information outweighs any potential impact to individual privacy. Any information input by a customer as part of a query, or by an individual for purposes of verifying their identity, is only used for that purpose (as well as legally required recordkeeping) and for no other purpose.

3.2 Will the information be shared with other individuals, federal and/or state agencies, private-sector organizations, foreign governments and/ other entities (e.g., nonprofits, trade associations)? If so, how will the vendor share the information?

Refer to the Equity Study PIA Section 4.2 "Will GSA share any of the information with other individuals , Federal and/or state agencies, or private sector organizations? If so, how will GSA share the information?"

TransUnion

Transaction information will not be shared with any third party.

Transactional (i.e., requested by public Internet users) CUI data will be deleted from TU vendor systems within 24-hours of the transaction time-frame and are not shared with any other third

party, except as required by law, outside of the purpose of the transaction (i.e. identity validation as requested by the user).

In the performance of the identity validation transaction, TU uses AuthenticID. IDVA interconnects directly with this vendor for the purpose of capturing driver's license and selfie images.

AuthenticID is not permitted to share data with any other third party by contract with TransUnion. Privacy and security of all third-party components are evaluated by the TransUnion Third Party Risk Management (TPRM) framework requiring documentation review, walk-throughs and on-site visits. TPRM processes are in turn reviewed by TransUnion's financial statement auditors who assert the adequacy of controls.

Socure

Yes. Socure relies upon a minimal number of service providers that provide verification and insight services with regards to the submitted PII. Socure hosts those solutions (i.e. datasets or services) internally and hence does not need to transmit the PII externally.

Jumio

Jumio will only share or provide access to the information in accordance with documented instructions from GSA. Jumio provides access to the data to GSA via the Jumio customer portal, which uses role-based access rules ensuring only GSA stakeholders are granted access to the data.

Incode

Incode will adhere to GSA's Zero Data Retention Policy. Incode leverages third parties for reading the text and barcode contents of the state-issued identification; neither of these services retain data. Since Incode and its partners do not store any data, there is no data to sell, market, share, or otherwise use for enrichment purposes.

red violet

Red violet does not share information external to the red violet, except with red violet's credentialed business customers who agree to limitations on use and applicable security requirements or as required by law. Red violet will engage with GSA to determine which information, and how much information, GSA will access (consistent with individual privacy expectations and privacy best practices). Information from GSA's query will not be shared with any third party and no PII will be stored by red violet.

3.3 Is the information collected directly from the individual or is it taken from another source? If so, what is the other source(s)?

Information is collected from both participants and vendor processing of participant-furnished information sources. For example, a participant will provide a picture of their identity document and a vendor will extract the machine-coded address and other information contained in the ID's barcode. Refer to Table 1 in Section D for a detailed listing of data sources.

TransUnion

The following information is collected directly from the participant:

- Images of the government ID
- Image of the participant selfie

Socure

IDVA and Socure collect, directly from individuals, all Identifiers and Geographic Data it requires for onboarding—e.g. first and last name, email address, current and past billing and mailing addresses, phone number, date of birth, physical or mailing address, and IP address. IDVA transmits data elements it collects to Socure via API. In addition to data received from the agency, Socure also collects the information outlined in its Products and Services Privacy Statement, including Device Information such as device geolocation, Government-issued identity documents, and Face Images and Data, including biometric identifiers. Socure conducts an assessment of each data point passed by GSA and returns a response indicating the likelihood the identity is authentic, the riskiness of specific pieces of PII, and the strength of the correlation between pieces of PII. Data is shared with the agency in accordance with applicable privacy laws and any relevant contractual provisions.

Jumio

GSA will collect information from the participant including images of documents and Selfies and submit them to Jumio for review. Jumio will determine whether a collected ID is fraudulent by looking at the features of the ID and using AI to review for manipulation and then comparing the individual selfie against the ID. See 4.1 for more information on the AI system.

Incode

Incode collects information directly from the participant after the participant provides expressed consent directly to GSA. As described above, the participant takes a photo of the front and back of their credential, and Incode's document authentication technology runs over 25 checks to ensure the credential is valid and unaltered. The facial image on the credential is converted into a binary template, or a string of code representing the face that cannot be

reverse engineered. The participant then takes a photo of their face. Incode's passive liveness technology ensures the person is a real, live person and not a video, mask, or other impersonation attempt. The selfie image is also converted to a binary template and compared to the binary template of the facial image from the credential to confirm a match. Incode Omni has been designed to only allow photos from the camera sensor. All photos are digitally signed and encrypted before images are transmitted over an HTTPS secure channel. Incode Omni does not offer the capability to access the device's file system or use other image sources during the photo process.

red violet

The information that red violet will collect from the user will be the PII claims the individual makes and send to us via the GSA equity study. Red violet will not collect any other directly from the individual. As described above, this information will only be used for the verification process and will be discarded after the verification process is complete.

The information red violet uses to verify the PII claims includes authoritative information sourced from:

- Credit Headers from Multiple Bureaus
- Public Records
- Government Authoritative Sources
- Consumer consented information from Commercial and Proprietary sources.

Having multiple data sources helps Red violet and its customers validate the relevancy and actionability of each Identity claim submitted by the individual.

Non-Federal SECTION 4.0 DATA QUALITY AND INTEGRITY

4.1 How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?

TransUnion

This system will collect information directly from the participant using technology designed to activate a mobile device camera (as permitted by the participant) in the form of a government identification document.

The system will not maintain the data for longer than 24 hours.

CUI data will be provided by public Internet consumer users via the IDVA system. TransUnion services will validate the input data for comparison to authentic identity records. Software applications use entity resolution logic to validate the comparison process the results of which are reported in real-time to the IDVA system.

Machine learning models are used within the process to improve accuracy and increase performance. PII and any associated images are not retained for this or any other purpose. Models will not be trained with the GSA participants data.

The data collected and pulled from the documents is passed back to IDVA for further verification of accuracy and completeness.

Socure

Socure performs various automated validation checks and normalization techniques before performing Socure's ID+ verification services. This includes assessing the entries for the possibility of mis-typed information, which is common when typing out names, or for transposed digits, which is common when typing out dates and numbers. Socure then checks the identifiers against authoritative data sources (e.g., credit bureaus, mobile network operators, and/or public agencies), as well as correlating user-entered PII against PII in the government identity document. In sum, identity verification by its nature is a process of checking for accuracy and completeness.

On machine learning training: Socure's machine learning models are trained on approximately four years of historical performance data across our consortium of clients from a range of industry sectors. Then, they are validated and tested on independent datasets. Socure conducts rigorous governance over its model development process (model components, development techniques, intended implementation and use, and change management processes), as many of its customers are subject to the financial services model risk management supervisory framework. Socure customers also provide ongoing feedback as to the performance of Socure services, which are also used to fine-tune our models' performance.

Notably, personal information submitted to Socure as part of the equity study will not be used for training models as described above, as GSA has specifically prohibited the retention of such data.

Jumio

GSA End-User PII is not used to train or support Jumio machine learning models.

Jumio processes the information automatically with the use of Jumio software and machine learning capabilities. Jumio applies the following criteria:

- Checks on the integrity and quality of the photographs;
- Checks on the integrity and recognition of the document;
- Extracting and analysis of text, graphical layout, and any other available information on the document, photographs, background;
- Analysis of results of all the steps combined;
- Lookups against known images as well as known cases of fraud;
- Your selfie is compared to the photo on the document.

In addition, Jumio takes the following steps to minimize demographic bias in algorithms:

- Uses large and representative datasets for accuracy across geographies; the model is trained on well-distributed global Jumio data with different genders, ages, and ethnicities;
- Trains AI models on real-world production data, not purchased data sets; and
- Builds in quality controls to maximize accuracy to prevent incorrect data from being baked into the AI models.

Jumio focuses on reducing bias not only from a technology perspective but by also diversifying the team that builds and works with AI models. Jumio employs a diverse team of verification agents and AI engineers from a variety of nationalities, genders, ethnicities, professional experiences, and academic backgrounds. Focusing on the team helps Jumio examine problems from different perspectives, which helps reduce demographic bias.

Incode

Incode's fully automated solution is highly accurate to ensure maximum identity assurance while maintaining privacy.

Participants take a photo of the front and back of their ID credential. Incode maintains a template library of over 4,600 document types, including all US driver licenses and identification cards. Within seconds of capturing the photo of the credential, our technology checks over 25 different features to ensure the credential is real and unaltered. Additionally, Incode uses optional character recognition (OCR) to extract data from the front of the credential and compares that data to the data contained within the machine-readable zone

(MRZ) of the two-dimensional barcode on the back of the credential. The participant then takes a photo of his face (a selfie). Incode's passive liveness technology ensures the person in the selfie is a real, live person. The photo on the ID and the selfie are each translated into binary templates, which are mathematical representations of the face that cannot be reverse engineered. Incode's software compares the selfie template and the ID photo template to confirm a match. Incode does not store or keep the photos that are captured in the process.

Incode has several built-in functionalities to ensure data integrity, accuracy, and completeness.

- Incode's facial recognition technology converts photos into binary templates. Binary templates are mathematical representations of the face that increase the accuracy of the facial recognition comparisons. Binary templates cannot be reverse engineered, ensuring that the identity is protected.
- Incode employs machine learning, computer vision, and AI on the edge (i.e., on the device itself) during the identity proofing process. Incode's fully automated solution greatly outperforms human adjudication and enhances privacy and accuracy, while ensuring the fastest, most secure process for the participant. Incode continually trains its model to further enhance accuracy. No new machine learning and/or labeling will occur using data from Equity Study participants.

Incode will delete all data, including both the photos and the binary templates, after transmission to GSA's system to adhere to GSA's Zero Data Retention Policy. As Incode will not store any data, Incode inherently lacks the ability to sell, market, share, or otherwise use participant information, including for enrichment purposes.

red violet

Red violet takes commercially reasonable efforts to ensure the accuracy of data existing within the system. Red violet's processes include machine learning and obtaining multiple sources for data points to ascertain consistency across the data set. Data existing within the system is obtained from public and proprietary data sources, as explained above. Red violet ingests this data and then employs AI and ML algorithms to establish identities using the multiple, disparate data sources. The AI and ML algorithms establish the identity based on the entropy of the identity (how the identity changes overtime), completeness of the identity based on linkages, and the veracity of the sources.

Data that is submitted by a customer or by an individual to verify their identity claim is only used for verification purposes. verification process. This information, as described above, is not stored or used for any other purpose. For the GSA equity study deployment, red violet will

process the data sent by GSA for an Identity Verification check; once the process is completed, the data will be discarded after the verification process is complete.

Non-Federal SECTION 5.0 SECURITY

All third parties have provided the required deliverables and artifacts as required in the Identity Proofing Equity Study Vendor Request for Information (RFI) on SAM.gov. These artifacts have been reviewed to determine the level of risk associated with using the non-federal systems to conduct the equity study and the effectiveness of the non-federal systems security controls in satisfying the requirements.

GSA Authorizing officials and CISO have determined the risk to GSA's systems, data, and/or assets resulting from the limited usage of these services for the Equity Study is acceptable.

5.1 Who or what will have access to the data in the system, application, or project? What is the authorization process to gain access?

TransUnion

Participant data will be accessible by vendor administrative users who have been authorized with such permissions as restricted data users. These users access such information only to troubleshoot or resolve issues with the functioning of the information system. Participant data will be evaluated by software located within vendor system boundaries designed to evaluate government identification documents for authenticity. Note that 24 hours after data collection participant data will be deleted and no longer accessible by these users.

Prior to issuing system credentials and granting access to the system or data, users are registered and authorized. The system authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.

Socure

Socure's ID+, including the Document Verification product, is an automated system that does not require human intervention. Individuals are not subject to the scrutiny of Socure employees as they are being verified by Socure's system. No humans assess the submitted PII before the Socure response is returned to the agency.

For purposes of maintaining Socure's services, certain authorized personnel have technical and role-based access to PII in ID+. GSA authorizes these staff to only access participants' PII information for these purposes:

- Technical implementation and operation of the API
- Quality control, such as testing in preparation for new/changed implementations or new/changed use cases
- Inquiries about particular transactions and why they returned certain recommendations, scores or codes, including for the purpose of studying fraud patterns and bias
- Ongoing improvements to product performance in order to continually react to, and prevent, new fraud attacks and fraud trends. This requires analytics studies and model development by data scientists. Their access to data and systems is based upon the principles of least privilege and role-based access.

Pursuant to Socure's Access Control Policy, users shall only receive necessary access privileges to services, applications, and other applicable systems required to perform their prescribed role and job duties. Any requests for additional access require approval from the employee's manager and Socure's Governance, Risk, and Compliance (GRC) team.

Jumio

Only Jumio employees with a need to know and have been authorized are granted access to the AWS cloud environment that hosts the solution or the web admin portals. GSA can register their own staff for access to the web customer portal.

Jumio ensures that all its personnel responsible for supporting services provided to GSA are securely authenticated and authorized before being granted access to any available GSA data. As GSA deletes the data after a transaction via the API, Jumio will not have further access to any PII data.

Authentication data such as passwords are not stored in a form that allows the authentication data to be recovered in readable or decipherable form.

Incode

GSA owns and controls its data. Incode will delete all data after transmission to GSA in order to adhere to GSA's Zero Data Retention policy. Incode follows the principle of least privilege (i.e., user is given the minimum levels of access needed to perform their job) using Role Based Access Control (RBAC), and has established defined steps to request, grant, and revoke access.

Usage is recorded, with logs containing source and destination IP address, username, date, time, and action performed. Once an Authorized Personnel no longer requires access to the data, the access is revoked. Access privileges are reviewed on a quarterly basis.

red violet

Only red violet's qualified employees will have access to systems that will be processing the data. These employees are system engineers who maintain the operability of the system. Data will at no time be stored on these systems and system engineers will not have access to data. Access is granted at the least privilege level and consistent with SOC 2, Type 2 standards and ISO 27001. Access is terminated immediately once no longer needed or through monthly access reviews.

5.2 Has a System Security and Privacy Plan (SSPP) been completed for the information system(s) or application?

Yes. Refer the Equity Study PIA Section 6.2 "Has GSA completed a system security plan for the information system(s) or application?"

TransUnion

AuthenticID has certified the system to American Institute of CPAs (AICPA) SOC2 Type 2. This includes an audit of internal controls, and an independent report on how well those controls are operating. This report has been shared to GSA for review. AuthenticID has also provided documentation supporting the implementation of GSA identified critical controls.

Socure

Socure has developed a System Security and Privacy plan (SSPP) in collaboration with GSA. This SSPP has been assessed by an independent assessor. Socure will continue to remediate identified deficiencies and work with GSA to provide the artifacts required.

Jumio

Jumio has created a System Security and Privacy plan (SSPP) in collaboration with GSA. Jumio maintains a written Information Security Policy and communicates it to all Jumio personnel and all other third-parties permitted to have access to the GSA's data or Jumio systems.

Incode

Incode has certified the Omni Identity Platform to AICPA SOC2 Type 2. This includes an audit of internal controls, and the development of a report capturing how Incode safeguards customer data and how well those controls are operating. This report has been shared to GSA for review.

red violet

IDI has documented policies, processes, and active efforts that adhere to this requirement. IDI will document those in a single SSPP plan. IDI has completed an initial System Security Plan and will add the privacy components to this plan and include any additional controls recommended by GSA. Red violet has a comprehensive set of policies and procedures that ensures continuous improvement and assessment of our security posture. IDI and red violet comply with ISO 27001 and SOC2 requirements.

5.3 How will the system or application be secured from a physical, technical, and managerial perspective?

TransUnion

The system is assessed by an AICPA third party against both ISO270001 and SOC 2. The system is designed and developed with security in mind and runs on a FedRAMP authorized cloud platform. Multifactor authentication is required for all privileged access or for access to sensitive data. Data is encrypted at rest and in transit. Vulnerabilities are identified and remediated in accordance with company policy and vetted by independent third party assessment. Personnel with access to sensitive information are subject to background investigation procedures in accordance with a documented and vetted onboarding policy. The system implements the concepts of least privilege and segregation of duties and audits user activity. The system Client side code is scanned and reported upon. Data retention policy is set to 24-hrs.

Socure

The production infrastructure for the in-scope application is hosted by Amazon Web Services (AWS). AWS is responsible for providing physical safeguarding of IT infrastructure, to prevent unauthorized access to the IT infrastructure. AWS is also responsible for providing environmental safeguards (e.g. power supply, temperature control, fire suppression, etc.) against certain environmental threats. As part of its cloud hosting services, additional AWS responsibilities include managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the online identity verification system resides.

Socure's network architecture places externally accessible resources, such as GSA's facing application's front-end, in a "public" subnet Security groups are configured in AWS to filter unauthorized inbound and outbound network traffic from the internet.

Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental design of ID+ are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role
- Use of encryption technologies to protect data both at rest and in transit

Access, Authentication, and Authorization

Authorized user account and password, with minimum password settings, MFA, and/or SSO authentication are enforced at production environment layers. In order to access the production environment for infrastructure that resides in AWS, users must first authenticate remotely via a VPN that enforces multi-factor authentication (MFA) that is integrated with Okta SSO. Once authenticated to the production environment users may SSH to a production server. Users authenticate to databases through a username and password once they have authenticated to a bastion (jump) server. Administrative access to the production environment devices, servers, database, and application are restricted to user accounts accessible by a limited population of authorized personnel.

Access Requests and Access Revocation

Management has established security controls so access to production systems is restricted to those who require access based on a valid business need. A formal provisioning process has been established for managing user accounts and controlling access to production resources. User access requests to production systems are documented in a request ticket and require the approval of a manager or HR prior to access being granted. The ability to create a new user or modify an existing user's access, is limited to authorized personnel.

In the event an employee is terminated, HR sends a notification within the HR system, which triggers access removal to the corporate environment, inherently invalidating access to the production systems. This also sends a notification to IT to manually remove users from systems within the production environment. Once the termination notice is received, access revocation requests for that employee are completed and access is revoked for employees as a component of the employee termination process. In order to confirm user access to the service is appropriate, user access reviews are performed on a quarterly basis of the AWS environment, google (e-mail directory) Okta SSO, and the application so access to the production systems is restricted to authorized employees.

User entities are responsible for adding/modifying/deleting designees on their respective instances. Additionally, user entities are responsible for ensuring that their users have appropriate access levels.

System Security and Monitoring

Documented standard build procedures as well as security and monitoring procedures, are maintained by Socure to guide personnel in the creation, installation, maintenance, and monitoring of in scope systems.

AWS security groups are utilized to control inbound and outbound traffic from production systems (using allow-listed IPs, network address translation (NAT), etc.) These security groups and NAT configurations are set to deny network connections that are not explicitly authorized. Administrator access privileges to configure the perimeter protections are restricted to user accounts accessible by authorized personnel.

Socure utilizes various tools / systems for its network services and monitoring processes. These tools collectively monitor system access, security metrics, resource utilization, availability/uptime, and performance metrics. The monitoring tools are configured to send alerts to IT personnel when predefined thresholds are exceeded on monitored systems. The issues identified and alerted by the monitoring tools are automatically logged in a centralized communication channel that is visible to IT operations personnel. A ticket is opened in the centralized ticketing system by the IT operations team for major issues, which is used to manage, record, and track identified system changes.

A central antivirus application is in place and configured to detect and prevent malicious code from being installed on production servers. The application utilizes advanced artificial intelligence (AI) and behavioral analytics to predict whether files contain malicious software in real time. In the event that an abnormality is detected, the system will alert the IT operations teams as well as automatically block the suspected malicious file. The antivirus software monitors both employee workstations and the production Linux servers.

In addition to ongoing system monitoring, vulnerability scans are performed on production servers on a weekly basis to identify potential vulnerabilities that need to be addressed. Furthermore, an authenticated penetration test of the production environment is performed by an independent third-party on an annual basis to identify potential security vulnerabilities. Points of concern or vulnerabilities found from both the vulnerability scans and penetration tests are followed up to resolution by the security team according to criticality and applicability.

Encryption

Web communication sessions between Socure and end users are protected utilizing TLS encryption for web communication sessions. In addition, production databases are configured to be encrypted at rest. All data in transit, including PII flows, are encrypted using TLS 1.2.

Third Party Services

Socure's Governance Risk and Compliance (GRC) team conducts vendor/contractor/service provider ("Third Party") risk management reviews prior to use and on an annual basis.

Jumio

Jumio uses commercially reasonable physical, electronic, and procedural safeguards designed to protect PII against loss or unauthorized access, use, modification, or deletion. Among other things, Jumio automatically encrypts sensitive information both in transit using TLS 1.2 and at rest with AES-256. Jumio regularly conducts security audits, vulnerability scans, and penetration tests to ensure compliance with industry security practices and standards.

Jumio registers and authorizes all users to their systems. Users are removed when access is no longer needed. Jumio implements concepts of least privilege and segregation of duties within its system and implements logical access controls within its software and infrastructure to protect information. Jumio monitors system access for indications of malicious or unauthorized behavior.

Incode

Incode has various technical controls in place, including web application firewalls, data encryption at rest and in transit, MFA, and segregation of systems. Incode logs all access to data and continuously monitors for suspicious activity. Incode regularly scans its systems and conducts annual penetration tests; identified vulnerabilities are monitored until remediation. Additionally, personal data is classified as confidential and encrypted both in transit (HTTPS with TLS 1.2 and TLS 1.3) and at rest (AES with 256-bit keys). Incode follows industry best practices and maintains SOC 2 compliance.

red violet

Red violet's Information Security Plan (ISP) focuses upon the following objectives:

- Confidentiality – Protecting the information from unauthorized access, use and disclosure;
- Integrity – Assuring the reliability, accuracy and completeness of information and IT resources by guarding against entry of unauthorized information as well as the modification or destruction of existing information; and,

- Availability – Defending information systems and resources to ensure timely and reliable access and use of information.

Red violet's ISP framework is a "Trifecta" model consisting of policies, standards and operational procedures and guidelines that includes all regulatory, physical and technical controls involved in the company's information security program. Collectively, these controls are summarized into fourteen domains which make up our ISMS:

- IT Governing Security Policies (Level 1) - describe the security objectives red violet wants to protect in terms of its information assets (i.e., data confidentiality, integrity, availability, regulatory compliance, etc.). Policies cover information security concepts at a high level, establish effective information security governance, define concepts, describes why they are important, and details red violet's stance on them. Our security policies and related controls are aligned with existing company-wide policies, best practice guidelines (i.e., ISO, NIST, SANS and ISACA), mandates (i.e., PCI-DSS) and applicable regulations (i.e., SOX, GLBA, OFAC, DPPA).
- IT Technical Standards (Level 2) - establish the acceptable boundaries for resources, processes and technologies in support of the IT Governing Security Policies (i.e., access control standards, patch management standards, encryption standards, etc.). IT Technical Standards describe specifically what must be done, or what parameters must be set, in detail, to achieve specific security objectives.
- Operational Processes, Procedures and Guidelines (Level 3) - practical documents that give step-by-step directions as to "how", "by whom", "when" and "where" to apply the IT Technical Standards (Level 2). They are written, owned and maintained by a variety of groups throughout the company, under the auspices of the Office of the CIO (OCIO).

Red violet's ISMS is process-oriented following the Six-Sigma DMAIC model (an acronym for Define, Measure, Analyze, Improve and Control) and complies with all International Organization for Standardization (ISO) requirements of its Information Technology-Security Techniques-Code of Practice for Information Security Controls (ISO 27002:2013). Applying this model, information security is optimized through continual analysis of data and information identified from risks, identified or suspected security incidents and information from other credible sources. Red violet's ISMS covers the fourteen domains identified by the ISO that are considered critical to IT security and GRC.

The above results in an implementation of best practice security processes and methods that include but not limited to:

· Configuring all systems to a secure baseline. Least Privilege is enforced throughout the system.
· Strong passwords requiring Multi-Factor authentication for access to all systems.
· Regularly scanning its systems for vulnerabilities, and managing/tracking their remediation.
· Regularly reviews audit logs for evidence of prohibited activity.
· Encryption of all data in transit and at rest.

In addition, IDI had been working with the GSA security team to implement the additional controls per their requirements. IDI will continue to implement those controls per GSA guidance.

5.4 What mechanisms are in place to identify and respond to suspected or confirmed security incidents and breaches of PII? If so, what are they?

TransUnion

AuthenticID has developed an incident response plan for their platform. This plan outlines what constitutes a security incident. It also outlines expectations for personnel and systems teams when responding to an incident, containment, and post incident activity. In the event of an incident involving GSA data, AuthenticID will notify GSA and coordinate its response activities.

Incident Response is a critical component of the TU Cyber Security program. Their Security Operations Center provides real-time monitoring and alerting on suspicious activity as part of their continuous monitoring program. Confirmed incidents follow a detailed response plan that would be escalated to specific TU leadership, and law enforcement and/or customers as determined by procedures based on the nature of the breach.

Socure

Incident response procedures are in place to address the reporting, classification, and handling of information incidents that impact the security or availability of the system or incidents that involve PII. Socure's Security Incident Response Policy and procedures are communicated to employees and are made available to employees via the company intranet. Socure's Incident Response Team manages the incident response process and there is at least one IT security technician on call to provide 24/7 availability.

Events and incidents are documented within the incident ticketing system for response and resolution. A business continuity and disaster recovery plan is in place and is tested on at least an annual basis. System support plans are provided to GSA and vendors for reporting security and availability incidents, concerns, and other complaints to Socure personnel. If an issue is identified, it is classified by the system on a priority level based on what the issue is, the severity of the issue, and whether it directly affected system availability. A containment, eradication, and recovery strategy is used to manage the incident and, if there was a high-risk issue, it would be noted and followed up to resolution. A security analysis is performed for any incidents which impact customer service.

The Socure Security Incident Policy describes the policy and processes to respond to suspected or confirmed security incidents or breaches, including incidents where PII may be involved.

Jumio

Jumio reviews logs of all key events (which may indicate security incidents leading to breaches of sensitive data) within Jumio systems and shall, upon identification of any material incidents and/or breaches regarding GSA End-User information, follow the GSA incident management requirements.

In addition, Jumio maintains a Information Security Incident Policy supported by an Information Security Incident and Data Breach Notification Procedures. These documents provide the foundation and processes for identifying and responding to security incidents, including breaches of PII.

Incode

Incode has a comprehensive Incident Response Plan for managing security incidents and data breaches. The plan includes steps for communications, monitoring, review, analysis, containment, investigation, escalation, and remediation of incidents. In the unlikely event that a security incident occurs, Incode will ensure that timely communications and close coordination of incident response activities between GSA and Incode will be strictly adhered to ensure successful notification, containment and remediation. Incode's Incident Response Plan is tested at least once a year.

red violet

Red violet maintains a detailed policy concerning confidential information breaches. The high level process is outlined below:

- Employees are required to report a breach to their manager and Office of the CIO (OCIO).
- Once reported, the manager will verify the circumstances of the breach, gather initial information, and inform the OCIO within twenty-four (24) hours with the initial report.
- Red violet's CIO or his designee shall act as the investigator of the breach. The CIO, or designee, shall be the key facilitator for all breach notifications to the appropriate entities.
- The CIO will take steps, if appropriate, to contain the breach.
- The CIO will maintain a record or log all breaches of confidential information.

Red violet will notify GSA of any breaches of confidential information if they occur as part of the GSA Equity Study. Red violet performs annual security roundtables to simulate security events.

Non-Federal SECTION 6.0 INDIVIDUAL PARTICIPATION

6.1 What opportunities do individuals have to consent or decline to provide information? Can they opt-in or opt-out? If there are no opportunities to consent, decline, opt in, or opt out, please explain.

Refer to the Equity Study PIA Section 7.1 "What opportunities are available for individuals to consent to uses, decline to provide information or opt out of providing information? If no opportunities exist to consent, decline or opt out, please explain." for details.

TransUnion

GSA will manage user consent for the Equity Study prior to accessing the AuthenticID product.

Socure

For document verification, the Socure product displays a modal (this is a small pop-up window that disables the main window but keeps it visible; users cannot move forward until they take an action in the modal) with notice language and requests affirmative consumer consent via a checkbox. The modal lets individuals know that the Document Verification product will allow GSA and Socure to collect, use and retain their images, including deriving biometrics from the images, for identity verification purposes. Socure will delete participant data from their systems, in accordance with GSA's written agreements with Socure, within 24 hours of collection.

Jumio

Consent is configurable by GSA to meet their business rules. For purposes of the Equity Study, GSA will present a uniform statement to the participants prior to routing to the Incode system.

Incode

Consent is configurable by GSA to meet their business rules. For purposes of the Equity Study, GSA will present a uniform statement to the participants prior to routing to the Incode system.

red violet

A consumer who does not wish to use the system for remote identity proofing is under no obligation to use it. Red violet complies with applicable privacy laws, including the California Consumer Privacy Act (as well as other state-based comprehensive privacy laws after their respective effective dates).

6.2 What procedures allow individuals to access their information?

Refer to the Equity Study PIA Section 7.2 "What procedures allow individuals to access their information?" for details.

TransUnion

There are no procedures to allow participants to access their own information collected by the system. All data is transmitted to GSA but not retained by the vendor beyond 24 hours of the participant transaction.

Socure

Socure is not retaining any data for GSA, a procedure allowing individuals to submit access requests is not required.

Jumio

A Participant cannot request access to the PII collected during the Equity Study directly from Jumio because Jumio does not store PII beyond the length of the transaction.

Incode

In adherence with GSA's Zero Data Retention Policy, Incode does not retain any participant data. GSA will determine the process for participants wishing to access their information.

red violet

As described above, red violet will not be storing any Information provided by the individual as part of the GSA Equity Study. As such, the individual will not have an opportunity to access their information.

6.3 Can individuals amend information about themselves? If so, how?

Refer to the Equity Study PIA Section 7.3 "Can individuals amend information about themselves? If so, how?" for details.

TransUnion

There are no procedures to allow participants to amend their own information collected by the system. All data is transmitted to GSA but not retained by the vendor beyond 24 hours of the participant transaction.

Socure

No. The information given to Socure cannot be amended after submission. Socure cannot undo or redo identity verification transactions that have already occurred. Socure's transaction database is merely a record of historical transactions, maintained for audit and integrity purposes.

Jumio

Jumio reviews the ID and Selfie submitted directly by a participant. Once submitted, the information cannot be amended.

Incode

In adherence with GSA's Zero Data Retention Policy, Incode does not retain any participant data. GSA will determine the process for participants wishing to amend their information. Additionally, Incode does not have the ability to update information housed by authoritative sources.

red violet

As described above, red violet will not be storing any Information provided by the individual as part of the GSA Equity Study. As such, the individual will not have an opportunity to amend their information.

Non-Federal SECTION 7.0 AWARENESS AND TRAINING

7.1 Describe what privacy training is provided to users, either generally or specifically relevant to the system, application, or project.

TransUnion

All vendor personnel are required to annually certify review and accept vendor Privacy Policy. Both aspects are tracked and monitored.

Socure

All staff must complete annual privacy and security training. Socure's Governance, Risk and Compliance team provides privacy and security training at employee onboarding and annually thereafter. This includes testing to assure efficacy of the training.

Socure utilizes computer based training (CBT) modules to deliver initial privacy and security training, at onboarding, and annually thereafter. Appropriate privacy and security topics such as, but not limited to, Privacy Overview, Privacy vs. Security, Notable Privacy Regulations, Data Classification, Proper Handling of Consumer Data, Reporting Possible Incidents, Least Privilege and Need to Know are just a few of the topics that may be covered. These trainings are mandatory for all staff.

The CBT software also provides reporting modules that are managed by members of Socure's Governance, Risk and Compliance Department. Reports are generated on a semi-monthly basis toward ensuring compliance with new hire and annual training requirements. Failure to comply with this required training will result in actions including but not limited to reports to the employee's manager, loss of access to Socure Systems, and escalations within the Socure management structure such as disciplinary action up to and including termination of employment.

Jumio

Jumio employees and contractors complete privacy and security training annually. Jumio maintains records of completion and reserves the right to restrict access to systems and applications when employees or contractors have not completed required training. If an employee or contractor does not complete training within the required period, Jumio escalates to managers to ensure training is completed.

Incode

All Incode personnel undergo onboarding training that includes modules on PII and GDPR, and annual refresher training on privacy security awareness throughout employment. Additional training includes modules on privacy security, common threats, and social engineering

techniques. All training is documented and logged, and all Authorized Personnel with access to PII must go through an established access request process and are appropriately trained to handle PII. Failure of an Incode staff member to complete required training is escalated to their manager for action. Repeat offenders are sanctioned according to Incode's Code of Conduct. Incode has a dedicated Security and Privacy team that regularly delivers updates, tips, and information on security-related topics to all Incode personnel.

red violet

Red violet trains its staff on these important issues on no less than an annual basis. The training for appropriate staff includes:

- IT Security and Awareness
- Payment Card Information Data Security Standards (PCI DSS)
- Personally Identifiable Information
- Data Protection and Destruction

Violations of red violet's IT Security and Training Policy or of any directive in connection with the Policy will be investigated by the OCIO. If in the judgment of Human Resources and of the CIO any non-compliance with this policy was willful or blatant, the responsible user is subject to discipline up to, and including, termination. The employee may also be subject to criminal or civil penalties.

Non-Federal SECTION 8.0 ACCOUNTABILITY AND AUDITING

8.1 How does the system owner ensure that the information is only being used according to the stated practices in this PIA?

TransUnion

Vendor employs a broad range of internal controls designed to ensure compliance to applicable laws, regulations and standards. This includes policy that prohibits the use of customer data in a manner that has not been previously agreed in writing, which are fairly represented within this document. There are numerous external and internal audits conducted attesting to this posture. This includes ISO270001 and SOC 2, which are in conformance with this PIA.

There are numerous audits conducted with reports available upon request.

Socure

Socure has strict access policies and technical controls requiring that employees only use PII for Socure's identity verification and fraud prevention purposes. Socure does not have any business functions that use the PII for any other purposes, such as business development or marketing. There are severe consequences for unauthorized access or attempts at access to ID+. Moreover, Socure's systems are not designed such that those functions could even access ID+ and its PII.

Jumio

GSA has a contract with Jumio that clearly restricts the use of PII. In addition, Jumio regularly conducts security audits, vulnerability scans, and penetration tests to ensure compliance with this PIA.

Incode

Incode logs and monitors all access to our systems. Incode has implemented Data Loss Prevention controls to detect potential suspicious activity. Incode Omni has integrated our access logs into our SIEM tool to generate alarms of potential security events. Incode performs quarterly audits of system's access and privileges. Incode follows the principle of least privilege (i.e., the user is given the minimum levels of access needed to perform their job) using Role Based Access Control (RBAC), and has established defined steps to request, grant, and revoke access. Events are logged, with logs containing source and destination IP address, username, date, time, and action performed.

red violet

Red violet maintains multiple, relevant internal policies as outlined in Section 4. Since the data from the Equity Study is immediately deleted, the information can only be used for the purposes outlined in this PIA. In general, red violet's policies ensure that all sensitive data is controlled and protected against unauthorized access; all data is assigned an owner who is responsible for properly classifying that asset and identifying the appropriate security in accordance with the security policies, standards, guidelines, and procedures.

In addition, red violet logs all queries to the system, and reviews such logs continually to detect any potential misuse (and address any such misuse with the applicable party). Misuse is subject to punishment including termination of employment for employees and termination of access to the system for third-parties (as well as any applicable, legal action that red violet may pursue). Finally, no 3rd parties will have access to data received from GSA queries.

Appendix B: Rules of Use

The Equity Study on Remote Identity Proofing is administered by the U.S. General Services Administration (GSA) and the participating identity-proofing vendors. The study will test how one-to-one (1:1) remote identity-proofing methods like facial-verification technology perform across various demographics to determine if vendor identity verification capabilities meet equity standards across various demographics. This study will enable GSA to make a data-driven decision on whether to pursue facial verification capabilities, to determine baseline performance metrics, and to provide real-world identity verification pass rate data to the broader Federal community.

GSA will collect Personally Identifying Information (PII) during this study to verify your identity. This will include comparing a photo of your identity document with a live photograph of your face (a “selfie”). GSA will also collect demographic information from you.
These Rules of Use provide:

- Information on the Equity Study process and what you can expect from it,
- The terms under which you participate in the Equity Study,
- How GSA and its partners will use your information and your rights to that information, and
- The conditions that you agree to when you participate in the Equity Study.

Prior to participating in the Equity Study, you are required to agree to these Rules of Use.

1. Your Agreement

By accepting these Rules of Use, you agree to participate in a study that will test the software of multiple Identity Proofing vendors. Specifically, this Equity Study will test the performance of document authentication, biometric comparison (comparing your selfie to the picture in your identity document), and liveness detection of the participating vendors. In addition, the study will assess vendor performance on the non-biometric aspects of the National Institute of Standards and Technology (NIST) SP 800-63-3 guidelines for remote identity proofing. This will allow for a more informed comparison of drop-off rates, i.e., to what extent a successful or unsuccessful identity verification is caused by either biometric or non-biometric aspects of the process.

You agree that:

1. You are not a person under 18 years of age,
2. Any information you provide to us is complete and accurate,
3. The identity you claim when participating in the study is your own, and
4. You will comply with applicable local, state, and federal laws during the study.

You further agree that you will NOT misrepresent your identity or any information you present in the Equity Study, including through participant support channels.

GSA will post any changes to these Rules of Use to https://identityequitystudy.gsa.gov/rules-of-use. If the changes affect GSA's handling of your personal information or are otherwise deemed significant, GSA will notify you by email. If GSA cannot reach you by email, GSA reserves the right to contact you by other means, including postal mail. If at any time prior to the completion of the study should you no longer agree to these Rules of Use, Privacy Act Statement, Consent Forms, Privacy Impact Assessment, or SORN, you may contact us at identityequitystudy@research.gsa.gov or (202) 969-0772.

2. How will GSA use your information?

Table 1: Data collected by GSA and its uses

Data Collected	Data Use
Demographic Information (self-reported race, ethnicity, gender, age, income, education, and skin tone)	Used to look for trends in identity proofing results.
Email Address	Used to share compensation details at the end of study and needed by the survey platform. If participants agree, GSA may also contact them via email for future studies.
Participant Name	Used to share compensation details at end of study
Images of Identity Document (front/back)	Used for the "document authentication" identity-proofing step and check that the identity document is legitimate.
Identity Document Machine Readable Zone information (barcode)	Used to verify that the identity document is legitimate.
Identity Document Number	Used to verify that the identity document is legitimate.
Identity Document Issue Date and Expiration Date	Used to verify that the identity document is valid.
Face reference (picture from Identity Document)	Used to verify that the identity document is legitimate, as well as the "biometric comparison" identity proofing step to compare the participant's Face reference to their selfie.
First, Middle, and Last Name (from Document)	Used to verify the participants' identity matches the identity document.
Date of Birth (from Document)	Used to verify the participants' identity matches the identity document.

Data Collected	Data Use
Sex/Gender (from document)	Used to verify the participants' identity matches the identity document.
Address Street, City, State, Zip Code (from Document)	Used to verify the participants' identity matches the identity document.
Live image of your face (or "Selfie")	Used to verify that the Identification document belongs to the participant.
Participant-Asserted Address: Street, City, State, Zip Code	Used to verify that the participant is who they claim they are.
Participant-Asserted Social Security Number	Used to verify that the participant is who they claim they are.
Participant-Asserted Date of Birth	Used to verify that the participant is who they claim they are.
Participant-Asserted Phone Number	Used to verify that the participant is who they claim they are.
Phone Number matching the User identity	Used to verify that the participant is who they claim they are.
Unique Mobile Device Identifiers	Used to compute a risk assessment of the mobile device used by the participant to access the study.
IP Address	Used to compute a risk assessment of the mobile device used by the participant to access the study.
Device Geolocation (IP based)	Used to compute a risk assessment of the mobile device used by the participant to access the study.
Device-behavioral Information (how the device and its applications are used)	Used to compute a risk assessment of the mobile device used by the participant to access the study.
Identity Proofing Results	Used for determine demographic bias in data

GSA will share a de-identified dataset containing aggregated demographic and identity-verification results with Clarkson University's Center for Identification Technology Research (CITeR) who will analyze the results and assist GSA in producing a peer-reviewed publication. To explain proofing failures, this publication (with your consent) may include images of the selfies and profile pictures from your identity document (any other PII in your identity document will be redacted).

As stated above, this publication will assist GSA in making more informed decisions regarding identity-verification capabilities. The outcome will also enable GSA to provide more equitable access to diverse populations that need to prove their identity to obtain government services.

3. Recruitment Service

GSA will be working with Rekrewt, a recruitment partner, to engage up to 4,000 participants residing in the US and US territories to participate in the study. Rekrewt will post advertisements in social media and assist GSA with building different outreach materials. Rekrewt will also manage participants' compensation. To track compensation and ensure GSA meets the study's demographic needs, Rekrewt will receive your name and email address along with an aggregated and de-identified demographic quota status.

4. Survey Administration

GSA will use a licensed survey software, Qualtrics, to send you a survey asking for your demographic information (race, ethnicity, gender, age, income, and educational level). This information will help GSA understand if and how demographics impact the identity-proofing results of various remote identity-proofing solutions.

Survey responses are stored in the Qualtrics system for the purposes of managing quota requirements. GSA will also store the survey responses in a GSA-licensed Google Drive to correlate the demographic data with the identity-proofing results.

To track completion status, this system generates a unique ID for each participant. Upon completion of all study requirements, GSA will provide your name and email address to Rekrewt to complete the compensation process.

If you decide to terminate your participation after completing the demographics survey, GSA will retain the de-identified demographic information to study drop-off rates and the recruitment process.

5. Device Risk Information Collection

While you are using the study's web-based platform, GSA will collect hardware and software data as well as device-behavioral information (how you use the device and its applications) for device risk detection from the personal mobile device you use to complete the study.

6. Vendor Performance of Identity Proofing Document Authentication and PII Validation

If eligible, you will also help GSA test multiple vendors' document authentication software. You will go through an identity-proofing workflow that includes document authentication and PII validation.

The identity-proofing workflow collects the following personally identifiable information (PII):

- a picture of your identity document and attributes printed on the document,
- a picture of your face, and

- your Full Name, Social Security Number, Date of Birth, Phone Number, and Physical Address

GSA will direct all identity-proofing vendors to delete your data from their systems within 24 hours of collection. GSA will retain records of this study in accordance with GSA's retention schedule for Customer Research and Reporting Records and any other applicable federal records schedules.

During document validation, you will provide information to GSA's vendors so they may provide identity-verification services to GSA. Specifically, GSA will present unbranded capture screens for the identity-proofing vendors. Each vendor will collect information from you during the presentation of their designated screens, including a selfie, and validate the provided data. Vendors will transmit their results to GSA, and GSA will store those results on the GSA Google Drive.

During PII validation, you will provide information directly to GSA. GSA then shares that information with the applicable vendors for verification.

The final step is a security code check that ensures the device you used in the workflow is in your possession and owned by you.

All data collected by the identity-proofing vendors shall be deleted within 24 hours of the transaction with each vendor. PII deletion from vendors' systems is achieved by different mechanisms, and ensured through a contractual requirement.

7. Exit Survey

After the last step in the Equity Study, you will be redirected to a GSA-administered Qualtrics exit survey. The purpose of the exit survey is to gather usability feedback with the study. A copy of the exit survey results will be stored in the GSA Google Drive and Qualtrics.

8. Termination

Participation in the Equity Study is voluntary. If you do not consent to the Equity Study, you may not participate and no identifying information will be collected. Once your information is submitted at the conclusion of the exit survey, you may no longer terminate your participation. In any event, GSA will still protect your personal information consistent with GSA's Privacy Act Statement and System of Record Notice.

Information collected through the Equity Study will be retained subject to GSA's System of Records Notice, as amended. GSA will retain records of this study in accordance with GSA's retention schedule for Customer Research and Reporting Records and any other applicable federal records schedules.

9. Authorities

GSA is conducting the study pursuant to 6 USC § 1523 (b)(1)(A)-(E) and OMB Memo M-19-17.

10. Service Operation and Customer Support

The Equity Study operates with a high standard of service, both in service delivery and customer support.

Availability and Uptime

N/A

Participant Support

Participant support is available through identityequitystudy@research.gsa.gov or via voicemail at (202) 969-0772. When you request participant support, GSA will use any information you provide to address your question or comment, and may use your feedback to improve this or future studies or for other purposes as GSA sees fit. In doing so, GSA will never reveal your personal information outside of the Equity Study except as required by applicable law or as stated elsewhere in these Rules of Use.

11. Responsibilities of GSA's Partners

Identity proofing vendors will collect data during the workflow and share results with GSA, and GSA will prohibit further access to data upon receipt. The identity-proofing vendors will delete this data within 24 hours of your identity proofing transaction. GSA will provide the Recruitment partner your email address and name for compensation purposes via Google products. All vendors are required to protect your information in compliance with federal law and policy.

In designing this study, GSA assessed each vendor, the type of data and level of access they require to render services, and all potential risks of both GSA and the vendor's processes and applications. Based on these assessments, GSA entered agreements that minimize the data vendors receive while still accomplishing the goals of the study. For further information about GSA's partners' responsibilities see the Equity Study's Privacy Act Statement

12. Fees

You will not be charged any fees for your participation.

13. Representations, Warranties and Liabilities

Participation in the Equity Study does not create a contractual relationship between participants and GSA, nor between participants and GSA's vendors. The Equity Study is provided "as is"

and on an “as-available” basis. GSA and its vendors make no warranty that the study will be error free or that access thereto will be continuous or uninterrupted.
In no event will GSA or its vendors, provided they are acting within the scope of this agreement and in accordance with applicable Federal, State and local law, be liable with respect to any subject matter of this Agreement under any contract, negligence, strict liability or other legal or equitable theory for: (1) any special, incidental, or consequential damages; (2) the cost of procurement of substitute products or services; or (3) for interruption of use or loss or corruption of data.

You hereby warrant that (1) your participation in the Equity Study will be in strict accordance with these Rules of Use and all applicable laws and regulations, and (2) your participation in the Equity Study will not infringe or misappropriate the intellectual property rights of any third party.

14. General Provisions

Entire Agreement

These Rules of Use constitute the entire Agreement between GSA and you concerning the participation in the Equity Study, and may only be modified by the posting of a revised version on this page by GSA.

Disputes

Any disputes arising out of this Agreement and access to or use of the services shall be governed by federal law.

No Waiver of Rights

GSA’s failure to exercise or enforce any right or provision of this Agreement shall not constitute waiver of such right or provision.

Contacting GSA

If you have questions about these Rules of Use or any other aspect of the Equity Study, you can contact us at identityequitystudy@research.gsa.gov.

Appendix C: Privacy Act Statement

1. Introduction

This Privacy Act Statement explains how GSA and identity proofing vendors handle the Personally Identifiable Information (PII) that you provide during recruitment, eligibility screening, and participation in the Equity Study. PII includes information that is personal in nature and which may be used to identify you. The PII you provide in this Equity Study will only be used for the purpose of this study and future Equity Studies if applicable. GSA will protect your information consistent with the principles of the Privacy Act of 1974, the E-Government Act of 2002, and the Federal Records Act.

2. Authority

GSA is conducting the Equity Study pursuant to 6 USC § 1523 (b)(1)(A)-(E) and and 40 USC § 501.

3. The Purpose

The GSA "Equity Study on Remote Identity Proofing" will assess the impact of ethnicity, race, gender, income, and other demographic factors on the multiple components of identity proofing, which is the process of verifying that a person is who they say they are. GSA will test remote identity-proofing tools that include both biometric checks using facial-verification technology as well as non-biometric methods like mobile-device account ownership and validating personal information through consumer reporting agencies. NIST's SP 800-63-3A guidelines for remote one-to-one identity proofing serve as a framework for the study.

To conduct this study, GSA is partnering with identity-proofing vendors that are compatible with the study architecture and can meet GSA's compliance requirements. The study will assess if and how demographic factors affect the vendors' remote identity proofing software's identity-proofing decisions.

4. What Information Does GSA Need?

4.1 General Information

- For recruitment, GSA needs your name and email address.
- For eligibility and to evaluate the equitable performance of technologies, GSA needs your demographic information, such as your race and ethnicity.
- For authentication, GSA needs your phone number to validate that you are an authorized user of the phone account and are in possession of the mobile device.

- To mitigate fraud, GSA will also analyze the device used to access the study, and collect different device identifiers as well as measures of behavior such as how you interact with forms on the page.

4.2. PII Validation

Identity proofing helps establish a person is who they claim to be and thus requires more sensitive information. One step in identity proofing involves PII validation, which will require the collection of the following data elements by multiple vendors:

- Participants' Full Name,
- Social Security Number,
- Date of Birth,
- Phone Number,
- Physical Address,
- the data printed or encoded (barcode) on your Government Identification card (e.g. driver's license)

GSA will facilitate the collection and transfer of this personally identifiable information (PII) to the following vendors, and you may review their privacy policies at the following hyperlinks:

- Privacy Policy | LexisNexis Risk Solutions Group
- Privacy Policy | Interactive Data (ididata.com)
- Socure Products and Services Privacy Statement - Socure

NOTE: The privacy policies above apply to the vendors' general commercial services, your data will be only retained and used in accordance with this GSA Privacy Act Statement.

For a detailed description of the information collected, its uses and protection, review the Equity Study's Privacy Impact Assessments (PIA) | GSA.

4.3. Biometric Information

In this study, GSA will also collect certain biometric information from you with the help of several vendors. This includes the following information used to identify you:

- Biological characteristics derived from a picture of your face (a "selfie"); and
- Biological characteristics derived from a photo of your identity document, which also contains a photo of you.

Vendors will collect this information and send it to GSA after assessing it as part of the identity-verification process. The vendors verify the identity document and match your photo from the document with your live selfie. The software will then validate your PII.

For more information on each provider's privacy policies, see the vendor's specific Privacy Policies.

- GSA | Incode
- Jumio's Privacy Notice - Jumio: End-to-End ID, Identity Verification and AML Solutions
- Privacy Policy | LexisNexis Risk Solutions Group
- Socure Products and Services Privacy Statement - Socure
- TransUnion LLC Privacy Notice | TransUnion

NOTE: The privacy policies above apply to the vendors' general commercial services, your data will be only retained and used in accordance with this GSA Privacy Act Statement.

4.4 Final Report

After the third party vendors determine whether you pass or fail their identity proofing, the vendors will share their results with GSA. GSA will group this data with your demographic information, remove any Personally Identifying Information (e.g. name, Date of birth, SSN), and share this report with researchers at Clarkson University and the Center for Identification Technology Research (CITeR). CITeR will help GSA perform a statistical analysis of the data, analyze failure cases and reasons and develop reports based on the Study's findings and data. All data will be securely stored in a GSA-licensed Google Drive. GSA will only transfer de-identified data to the CITeR through secure means like SFTP, file share, or read-only Google Drive file share.

This study and the associated reports will assist GSA in making informed decisions regarding commercially-available identity-verification capabilities and enable GSA to provide equitable access to diverse populations that need to verify their identity to access government services.

5. Retention of Data

GSA will instruct all vendors providing identity proofing services for this study to discard any information collected within 24 hours of collection. GSA will retain records of this study in accordance with GSA's retention schedule for Customer Research and Reporting Records and any other applicable federal records schedules.

Recruitment Partner/Participant Outreach Service Vendors will retain the data for 90 days after the Equity Study and then delete the data. No PII will be retained by the vendors at the conclusion of this study.

CITeR will not collect or store PII for the Final Report, except that, with your consent, your redacted images may be included in the Final Report to explain proofing failures; if included (with your consent), images of identity documents will be deidentified to the greatest extent possible in the report.

6. Additional Information Sharing

There may be circumstances where GSA is required to share certain data. For example: if the information is relevant and necessary for an authorized law enforcement purpose; in order to respond to a breach; or to assist another agency as it responds to a breach. For additional information, see the system of record notice number GSA/TTS-1 that GSA's Technology Transformation Service (TTS) published on November 21, 2022.

7. Routine Uses - With whom will the information be shared?

To third-party identity proofing services and fraud prevention services when participating in studies commissioned by the GSA to evaluate the equitable performance of new technologies and guide service improvements. Please refer to the System of Records Notice, GSA/TTS-1, for the full list of routine uses, which represent the authorized entities GSA may disclose the information to, as determined relevant and necessary.

8. Consent - How can you control what information is shared?

Participants in this study have consented to the collection and use of the information as described in the Rules of Use, Privacy Act Statement, Consent Forms, Privacy Impact Assessment, and SORN. If at any time prior to the completion of the study should you no longer agree to these conditions, contact identityequitystudy@reseach.gsa.gov or (202) 969-0772.

9. Records - Where can you find more information?

Please see the GSA System of Records Notice, GSA/TTS-1.

10. Website Analytics – Other data GSA collects

Other data, like the pages you visit and the length of your session, are aggregated into reports to help us better understand how the site is being used and how GSA can make it more helpful. The data is anonymized. No personally identifying user information is tied to this data and it is only shared anonymously with the GSA team.

11. Privacy Impact Assessment

View all GSA privacy impact assessments at www.gsa.gov/PIA.

12. Contact Information

If you have any questions regarding GSA's Privacy Act Statement or the use of your information, please visit www.gsa.gov/privacygsa or contact GSA.privacyact@gsa.gov.

OMB No: 3090-0328
Expires 05/31/2026

Paperwork Reduction Act Statement - This information collection meets the requirements of 44 U.S.C. § 3507, as amended by section 2 of the Paperwork Reduction Act of 1995. You do not need to answer these questions unless we display a valid Office of Management and Budget (OMB) control number. The OMB control number for this collection is 3090-0328. We estimate that it will take up to 45 minutes to read the instructions, gather the facts, and answer the questions. Send only comments relating to our time estimate, including suggestions for reducing this burden, or any other aspects of this collection of information to: General Services Administration, Regulatory Secretariat Division (MVCB), ATTN: Lois Mandell/IC 3090-0297, 1800 F Street, NW, Washington, DC 20405.

Appendix D: Consent Language

Part 1 - Study Steps and Registration

<Participants will arrive at this screen after clicking on a link in the Equity Study Webpage, or a social media advertisement or email from GSA's participant-recruitment partner>

Welcome to the GSA Equity Study on Remote Identity Proofing

Thank you for your interest in the General Services Administration (GSA) Equity Study on Remote Identity Proofing. GSA appreciates volunteers like you who are helping improve government services for the American people.

Identity proofing is a way of providing information about yourself to help someone, such as a government agency, verify your identity to confirm that you are who you say you are.. By participating in this study, you will help inform decisions on using new technologies to interact with government agencies online.

Accessibility
GSA recognizes that the "Equity Study on Remote Identity Proofing" may not be accessible to all potential participants with disabilities because it requires participants to take photographs of their government-issued ID as well as a live "selfie" or headshot using functionality that may not be native to their device. GSA is investigating other remote identity proofing solutions that are designed to be more accessible and compliant with the requirements in National Institutes of Standards and Technology (NIST) Special Publication (SP) 800-63.

[NEXT BUTTON]

Study Purpose and Participation Requirements

GSA will publish a de-identified, peer-reviewed report assessing the impact of ethnicity, race, gender, income, and other demographic factors on identity-proofing tools. You will test and provide feedback on multiple identity-proofing components and products including:

1. Document Authentication

- You will take and submit pictures of your identity document (e.g., a driver's license, state ID)
- You will take and submit a "selfie" (a picture of your face)
- You will rate the "ease of use" of the tool
- You will repeat these steps for **FIVE (5)** different document authentication products

2. Personal Information Validation

You will provide your:

- Full legal name
- Date of birth
- Physical address
- Social Security Number
- Phone number

3. Device Checks

- You will receive and confirm a security code by phone (voice call or text message)
- This application will scan your mobile device and evaluate it for its capabilities, features, and uses.

4. Exit Survey

- You will answer three (3) short questions

Participant Acknowledgements and Agreements

With your consent, GSA will share your information with third party vendors who will only use it to verify your information. GSA will collect and store your data along with the vendors' validation and verification results. None of your data will be used for marketing or purposes other than this research.

GSA will instruct the vendors to delete your data from their systems within 24 hours of collection.

GSA will share an aggregated de-identified dataset with CITeR and Clarkson University for analysis. Your personally identifiable information (PII) will not be included in the data that GSA shares with GSA's research partners.

Your participation is voluntary. You can withdraw from the study or cancel your permission for GSA to use your identifying information prior to study completion by closing the study webpage on your browser or contacting the GSA researchers at identityequitystudy@reseach.gsa.gov or (202) 969-0772.

If you decide you don't want your information used, or if you have any questions or complaints, you may also contact a person not on the research team at the Biomedical Research Alliance of New York Institutional Review Board at (516) 318-6877 or at www.branyirb.com/concerns-about-research. Information that was already collected may still be used.

Risk and Harm: GSA and its partners are committed to protecting your data to the greatest extent. However, there is always the risk of loss of confidentiality of your personal information used for this study. If this were to happen, GSA will promptly inform you with additional information.

Please read the study's Rules of Use and the Privacy Act Statement.
<links open in new tab>

- I have reviewed the Rules of Use and the Privacy Act Statement and agree to abide by them.

*Are you interested in participating in the study?

- I am interested in participating in the study. I consent to the collection and use of my information as described above.
- I am not interested in participating in the study. I do not consent.

[NEXT BUTTON]
<If participant clicks "I am not interested" they get routed to the "not eligible" page, if they do consent clicking "next" will take them to the "Study Registration" page below.>

Study Registration

* Please provide your contact information. (This information will be used to notify the recruitment partner when you have completed the study, so they can follow up with you about compensation.)
First Name <ENTER VALUE>
Last Name <VALUE>
Email Address <VALUE>

[SUBMIT BUTTON]
<Participants provide name and email address and clicks "Submit" button they will receive an email with a link to a personalized survey, see Email for Demographic Intake**>**

Part 2 - Consent Screens in Identity Proofing instrument

<Participants will arrive at this screen if they are eligible after taking demographic intake survey >

GSA will ask you to capture images of your government-issued identity document, take several "selfies," and provide Personally Identifying Information (PII), including biometric data, to help GSA test multiple identity-proofing processes. The third-party vendors listed below will validate and verify your provided information to provide a "proofing score" for each of these steps. The remote identity proofing software will try to:

1. compare your "selfie" against the photograph in your identity document using facial verification technology *and*
2. compare your Social Security Number (SSN), name, date of birth, address, and phone number against different record systems.

Each vendor's policy is available below for your reference and review:

- Socure
- LexisNexis
- TransUnion
- Jumio
- Incode
- red violet

NOTE: The privacy policies above apply to the vendors' general commercial services, your data will be only retained and used in accordance with the GSA Privacy Act Statement.

GSA will instruct the vendors to delete the data you have provided within 24 hours of submission. GSA will collect and store your data along with the vendors' validation and verification results. GSA will share an aggregated de-identified dataset with CITeR and Clarkson University for analysis. **None of your data will be used for marketing or purposes other than this research.**

By selecting "I consent" below, you agree to the collection and processing of your personal information, including biometric information as described in Section 4.3 of the Privacy Act Statement, and you

acknowledge that you may choose to terminate your participation at any time prior to completion of the study for any reason.

- I consent.
- I do not consent. I do not wish to participate.

<If participants select "I consent" they will progress through the remainder of the collection instrument. If they select "I do not consent. I do not wish to participate" they will be directed to the "thank you" screen.>

Vendor-specific Consent

<One of the biometrics identity proofing vendors required the additional consent screen below>

Terms and Consent

For our service provider to verify your identity, click “I Agree” to:
- Agree to their Terms of Use (incl. Arbitration terms and class action waiver); and
- Consent to their collection, use, and retention of your biometrics and personal information according to their Privacy Statement

GSA Users Only: Your data will only be retained and used in accordance with GSA’s written agreements with Socure, notwithstanding the privacy statement linked above. Relevant terms of those agreements are outlined in the GSA Privacy Act Statement.

[**I decline**, BUTTON] [**I agree**, BUTTON]

<If participants click “I decline” data will not be collected for this specific vendor. Participants will be routed to the next vendor.>