Google drive location:
https://docs.google.com/document/d/1L_ZAZt4fhRlodcaRsu2iTC6STwZ5ndXS/edit?rtpof=true

Approvals

Name	Role	Signature
Laura Gerhardt	Acting Chief Privacy Officer	DocuSigned by: 9/16/2022
Jacqulyn Henry	Privacy Analyst	DocuSigned by: 9/12/2022
Micah Pischnotte	Technology Law	DocuSigned by: 9/16/2022
Ryan Palmer	ISSM	DocuSigned by: 9/17/2022
Cody Reinold	Delivery, Login.gov	9/16/2022

LexisNexis Risk Solutions (LNRS) Identity Proofing

Privacy Impact Assessment (PIA) - Guidance

September 15, 2022

POINT *of* CONTACT

gsa.privacyact@gsa.gov

GSA IT

1800 F Street NW

Washington, DC 20405

Instructions for GSA vendors:

This guidance is designed for nonfederal systems described in the National Institutes of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations". GSA requires vendors to conduct privacy impact assessments (PIAs) for electronic information systems and collections in accordance with CIO 1878.3 Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices. PIAs offer an opportunity for vendors to highlight the data protection, privacy by design, data minimization and similar principles that their services may employ.

Vendors may use this or their own templates/forms to meet the requirement. If vendors use their own template, GSA requires that vendors order their sections/responses consistent with the below questions for the benefit of GSA's customer agencies and for simplicity during the review process. The vendor must demonstrate how it collects, stores, protects, shares, and manages personally identifiable information (PII). The purpose of a PIA is to demonstrate that nonfederal system owners and developers have incorporated privacy protections throughout the entire life cycle of a system. GSA will publish the final product on its public website www.gsa.gov/PIA. Please review all questions and the bracketed guidance, then develop your response.

GSA Stakeholders

The GSA representatives listed below have reviewed the information provided by the vendor for completeness.

Name of GSA Information System Security Manager (ISSM): Ryan Palmer

Name of GSA Program Manager: Mossadeq Zia

Name GSA Chief Privacy Officer (CPO): Laura Gerhardt

Name of GSA Contracting Officer (CO): Marion Williams

800-171 PIA Template Version 1.4 (Released 12/1/2020)

Table of contents

DOCUMENT PURPOSE

OVERVIEW

SECTION 1.0 OPENNESS AND TRANSPARENCY

SECTION 2.0 DATA MINIMIZATION

SECTION 3.0 LIMITS ON USES AND SHARING OF INFORMATION

SECTION 4.0 DATA QUALITY AND INTEGRITY

SECTION 5.0 SECURITY

SECTION 6.0 INDIVIDUAL PARTICIPATION

SECTION 7.0 AWARENESS AND TRAINING

SECTION 8.0 ACCOUNTABILITY AND AUDITING

Document purpose

This document contains guidance for vendors that maintain and operate nonfederal systems. To provide the requested service, the vendor collects, maintains and/or disseminates 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.

Vendors should use this PIA guidance to explain how and why they collect, maintain, disseminate, use, secure, and destroy information in ways that protect privacy. This PIA comprises sections that reflect GSA's privacy policy and program goals.

A. System, Application, or Project Name:

The LexisNexis Risk Solutions (LNRS) identity proofing for Login.gov includes a workflow made up of solutions that will provide identity verification for individuals utilizing Login.gov for identity verification. The following solutions will be utilized:

- **Instant Verify:** A real-time verification service that validates if the subject identity exists. This service goes beyond standard wallet verification to provide date of birth, deceased, occupancy, high-risk address, and phone checks, amongst many other checks, returning an indicator that validates the information submitted.

- **Phone Finder Ultimate:** Uses authoritative phone content with the industry's largest repository of identity information to deliver relevant, rank ordered connections between phones and identities. Using the phone number, full name, and address, information is returned such as phone type, status, CallerID and portability information. This solution leverages proven analytics and proprietary scoring technology to determine the best subjects for an input phone or best phones for an input subject. Includes phone number spoofing capabilities in addition to information from third-party phone content providers

- **ThreatMetrix Device Assessment:** Profiles devices accessing the Login.gov website and the native mobile application, including desktops, laptops, smartphones, or tablets, to detect suspicious devices, spoofed IP addresses, and the presence of malware or other anomalies that might indicate a high-risk application. ThreatMetrix analyzes connections among devices, locations, tokenized identity information and intelligence and combines this data with behavioral analytics to identify high-risk digital behavior and transactions in real time.

- **ThreatMetrix Behavioral Biometrics**: Behavioral Biometrics provides the ability to collect and analyze risk signals based on how users interact with their devices (when accessing the Login.gov website), such as how they touch and move their devices. By analyzing these behavioral traits and patterns, ThreatMetrix is able to identify several indicators of fraud, social engineering, and remote access. Behavioral Biometrics has proven to correlate highly with bot activity and is extremely beneficial in other use cases across industries. As with all of the ThreatMetrix modules, all user PII data is obfuscated. The submitted PII is used to look up an existing LexID Digital and is a unique identifier based on anonymized global shared intelligence from the Network. This identifier is dynamically matched or created based on each individual transaction in the network; the LexID Digital engine takes care of merging previously disparate digital identifiers.

- **TrueID®:** A document authentication service that authenticates Government-issued documents submitted as part of the identity verification process. This service validates the authentication of the document by performing checks against a document template database containing attributes used to validate the authenticity of the Government-issued documents being submitted for proof of validation. The image is captured when the citizen submits the front and back of the document which then goes through optical character recognition and a validation to ensure the data that is visible on the ID matches the data that is encoded in ID barcode and the ID magstripe. If the data matches, it is less likely that the ID is fraudulent.

- **Emailage®:** A fraud prevention solution that uses email intelligence as a risk identifier. Emailage assesses risk by evaluating email address metadata points such as domain details, email details, risk indicators, and when available, other personally identifiable information. Emailage delivers a risk score providing validation of the email address being used in the transaction.

- **FraudPoint®**: Fraud detection solution that detects fraudulent applications including synthetic identity and other types of fraud. Leveraging authoritative consumer, business and asset content and advanced linking technology, FraudPoint gathers and analyzes hundreds of unique identity characteristics and life events to identify inconsistencies and fraud patterns in application profiles and the applying identity. FraudPoint examines the data interconnections to provide clear perspective into identity fraud and fraudulent applications and fraudulent events that are occurring.

B. GSA Client:

GSA's Technology Transformation Service (TTS) Login.gov.

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

LNRS is the identity authentication solution used to provide identity proofing of the subject of interest; to help the GSA client determine if an individual should be granted access to that clients' applications/benefits.

Individuals utilizing the Login.gov and LNRS identity solutions will be submitting their government issued document via TrueID whereby demographic data elements will be extracted from machine readable zones (MRZ) such as:

- name,
- address,
- social security number,
- driver's license number,
- phone number,
- date of birth,
- and passport number.

Login.gov will leverage:

- first name,
- last name,
- ID number,
- ID type,
- date of birth, and
- address across the workflow implemented.

Additionally, during the citizen transaction, attributes including the email address, IP address, device characteristics, keyboard strokes (alpha/numeric keys, passwords, and PII are not logged), mouse movement, touchscreen actions, and characteristics specific to the device identity being used will be captured and scored to assess risk based on the custom rules designed by Login.gov.

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

The chart below shows the data elements or attributes that are used by each LNRS product in the Login.gov workflow.

Solution & Data Elements Used	
ThreatMetrix	***TMX Behavior Biometrics***
Session ID	Keyboard Strokes (no alpha/numeric or passwords are captured)
Full Name	Mouse Movements
Address	Sensors
SSN	Touchscreen Actions
Driver License Number	
Phone Number	
Date of Birth	
Email Address	
Device Data	

(Identifiers for operating system, IP, browser,	
Instant Verify	***Emailage***
Full Name	Email Address
Address	IP
SSN	Last Name
Driver's License Number	First Name
Phone Number	Address
DOB	Phone
TrueID	***Phone Finder Ultimate***
Government Issued - Document Image - Front	Phone Number
Government Issued - Document Image - Back	Full Name
	Address
FraudPoint	
Full Name	
Address	
DOB	
SSN	

Phone Number
Email Address
IP Address

E. The purpose of the system, application, or project is:

LexisNexis is a third-party identity proofing service utilized by the Login.gov system. Identity proofing is the process of verifying that a person is who they say they are. PII must be collected from a Login.gov user to prove that user at an Identity Assurance Level (IAL) required by a partner agency to grant access to its information, applications, programs, or records (for the purpose of this PIA, ‘‘services’’). The National Institute of Standards and Technology (NIST) defines IAL as “a category that conveys the degree of confidence that the applicant’s claimed identity is their real identity.” Identity assurance levels categorize “the degree of confidence that the applicant’s claimed identity is their real identity.”

Additionally, Login.gov leverages LexisNexis fraud detection solutions as a fraud mitigation measure that delivers real-time, automated digital authentication which is critical in distinguishing a legitimate citizen from a cybercriminal, on the day the account is opened and for every subsequent transaction with Login.gov. LexisNexis provides Login.gov, a fast digital identity assessment, including data intelligence about devices, locations, identities and past behaviors across one of the world’s largest, crowdsourced, global digital networks. The result allows Login.gov to know who they’re transacting with, reducing access from fraudsters and bots.

SECTION 1.0 OPENNESS AND TRANSPARENCY

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

GSA owns a reusable identity credential that users can opt to share with other government agencies’ applications in order to receive a service. GSA relies on LexisNexis services to establish this identity credential by:

- Authenticating identity evidence provided by the user
- Detecting and preventing identity fraud

GSA also owns the interface that is collecting the data from the public and must provide any notices required before collection, maintenance, or use of dissemination of personal information. Please see Login.gov PIA at www.gsa.gov/PIA for additional details. LexisNexis performs no independent collection, maintenance, use or dissemination of personal information outside of the interface provided by the Login.gov interface.

SECTION 2.0 DATA MINIMIZATION

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

The collection and use of PII is critical and necessary in the identity proofing of individuals using Login.gov for identity verification. LNRS employees supporting the LNRS Identity Proofing solution will only have access to information about the transaction that was submitted for verification, but in a limited data capacity. They will have information such as transaction IDs, what checks failed, reason codes, and risk scores. These checks, reason codes and scores do not contain any PII and only provide indications into the nature of the failure or the overall risk score. An example of a reason code would be "The SSN does NOT match the First and Last Name", but no other information specific to an individual would be provided.

By combining multiple solutions into the Login.gov workflow, a comprehensive view of the identity, and method of submission of information, can be analyzed and evaluated for authentication. The submission of PII is required to validate the individual against the LNRS public records information. The PII data elements submitted allows LNRS to provide Login.gov with the ability to validate the identity or identify and flag false identities that may be used to conduct fraudulent transactions.

Utilizing Instant Verify, Phone Finder Ultimate, and the FraudPoint solution, the LNRS linking technology examines the PII submitted to provide a score that indicates warning codes for high-risk conditions or transactions. LNRS will retain the transaction ID, LexID, and Status/Code results from the transaction.

Email addresses submitted by the individual are validated using Emailage as another part of the workflow in validating the identity. The email address submitted is validated against prior use and historical data in the global digital network, in conjunction with the

name and address submitted that allow Login.gov to confirm the email address submitted for the transaction. LNRS will maintain the email address only as required for product functionality.

The use of ThreatMetrix Device Assessment and Behavior Biometrics captures information from the device being used in the transaction that allows for analysis of the device data, interaction data and related PII to provide indicators of a potential fraudulent transaction. These solutions provide BOT detection, identifying infected devices containing malware, and identify additional hidden elements that are used to recognize digital behavioral anomalies that signal potential fraud. LNRS will maintain the session ID, device data, score and reason code from the transaction for Login.gov anti-fraud purposes.

The use of TrueID allows Login.gov to validate the authenticity of the Government-issued ID (driver's license or other valid state issued ID) being submitted as part of the document authentication process. True ID uses the document front and back submitted by the individual to validate the type and format of the ID document being submitted. In addition to type and format, the document is validated for correct format, including data elements, are cross checked against known document sources to verify authenticity. The images used for these transactions are not maintained by LNRS, and/or partners, after the validation is completed. LNRS will maintain the transaction Id and optical check results for product functionality and performance.

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

The LNRS identity solution is used for identity verification for Login.gov credentials. The identity verification occurs only when the individual submits information in the use of verification of their identity. Login.gov and LNRS employees supporting the LNRS Identity Proofing solution will only have access to information about the transaction that was submitted for verification, and limited related data. They will have information such as transaction IDs, what checks failed, reason codes, and risk scores. These checks, reason codes and scores do not contain any PII and only provide indications into the nature of the failure or the overall risk score. An example of a reason code would be "The SSN does NOT match the First and Last Name", but no other information specific to an individual would be provided. This information will be used in the capacity of product performance and fraud analysis of transactions.

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

The reporting capabilities are transaction based and are not tied to an individual. Login.gov and LNRS employees supporting the LNRS Identity Proofing solution will only have access to information about the transaction that was submitted for verification, but in a limited data capacity. They will have information such as transaction IDs, what checks failed, reason codes, and risk scores. These checks, reason codes and scores do not contain any PII and only provide indications into the nature of the failure or the overall risk score. An example of a reason code would be "The SSN does NOT match the First and Last Name", but no other information specific to an individual would be provided.

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?

Login.gov and LNRS employees supporting the LNRS Identity Proofing solution will only have access to information about the transaction that was submitted for verification, but in a limited data capacity. They will have information such as transaction IDs, what checks failed, reason codes, and risk scores. An example of a reason code would be "The SSN does NOT match the First and Last Name", but no other information specific to an individual would be provided.

The PII and device data within the ThreatMetrix platform is used to look up an existing LNRS identity. The PII associated with LNRS identities is obfuscated in viewing reports.

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?

The information shared from Login.gov to LNRS is limited to only data that is needed to carry out the purpose of the collection. The limited data retained of session ID, device data, email address, keyboard strokes (alpha/numeric keys, passwords, and PII are not logged), mouse movement, touchscreen actions, and data related to the transaction are retained by LNRS is for the purpose of product performance and functionality.

3.2 Will the vendor share any of the information 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?

LNRS will only share the ID images required for processing the True ID transactions with a 3rd party that has been approved by GSA as part of this use case. The 3rd party will

process the data without any data retention occurring. The processing of data will occur over a secure FIPS 140-2 compliant transmission.

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)?

The LNRS solutions collect data via direct input from the individual, e.g. document image capture and keyboard entry as well as collecting device information via a javascript loaded on the Login.gov webpage. For device data, ThreatMetrix, collects device information along with the subject's behavioral biometrics from the individual's device upon loading the Login.gov PII verification page and subsequently collects information about the subject's interaction with the device when filling out the PII requested on this webpage. Common examples of attributes captured include data about the web browser, IP, mouse movements (position, off-page, etc.), cut/paste activity, time spent on a page or field, etc.

These device attributes and behavioral data are then sent in the request to LNRS the subject's collected PII. The subject's PII and document photo are then collected from the individual's submitted photo ID document issued by a Governmental Agency (such as a DMV) along with other PII elements that have been collected via the Login.gov 's PII verification page such as an IP address, and email address, phone number, and SSN.

The above collected information is sent to LNRS via a Restful API. The transport layer security is FIPS 140-2 TLS 1.2 compliant.

SECTION 4.0 DATA QUALITY AND INTEGRITY

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

The LNRS identity solution will crosscheck information and documentation submitted by the individual against several security checks to validate the authenticity of the information and documentation provided. Please see the following description of the various applications used within the identity proofing process employed by the Login.gov website powered by LNRS.

Using PII and device-collected attributes, ThreatMetrix checks against a global crowdsourced database to detect the global reputational awareness and fraudulent activities associated with the device and the Identity associated with the device. The PII is used to look up the LNRS identities in an obfuscated manner (one-way Hash) where no

one is able to ever see the PII submitted. Internal LNRS employees are unable to see the PII used for these products.

True ID, the application used in checking document authenticity, sends the collected information from LNRS to a 3rd party vendor via a secured API for verification of the authenticity of the document. There, TrueID auto-classifies the ID document, e.g., State of Virginia Driver's license, to identify its corresponding Document Library template with known expected security features. Using the known format, TrueID extracts the data from all visible fields and machine-readable zones (MRZ), comparing and cross checking all data (e.g. DOB may be in three locations). Proprietary algorithms then evaluate and assess all text and image-based test results to determine document authenticity and an overall pass or fail result is returned. The information from the document is not stored at the 3rd party vendor.

The PII contained in the barcode on the back of the verified authentic document is then used within the Instant Verify, FraudPoint, Phone Finder and Emailage products along with the other PII collected.

For Instant Verify, the submitted PII is checked to first confirm the existence of a subject within the LNRS public records database. Then, the PII is run through a series of configurable checks to confirm that each of the elements is verified for that identity, such as, does the submitted SSN match to the name and address submitted since the name and address pair came from the TrueID authenticated Government issued document and the SSN was submitted to the Login.gov verification page from the subject.

Emailage, in the same vein as ThreatMetrix, confirms the collected attributes against a global contributory database and provides a score as to the authenticity of the email. For example, these checks include the length of time the email has been in use or has the email been tagged as having a bad reputation within the global database.

FraudPoint uses the submitted PII and provides a score based on LNRS data models. The models look at metadata of the provided PII such as the number of LNRS sources that the PII comes from, was the SSN issued prior to the DOB, and are there relatives and associates associated to the discovered identity within our system.

Phone Finder uses the submitted PII and verifies that it matches the phone number provided and that the associated PII, e.g. name, address, are associated with the submitted phone number. The application also has a configurable number of checks with a configurable level of priority of them to determine if there are any risks associated with

the phone number, such as, has the SIM been swapped or ported, how long the phone number has been in use, is the phone a prepaid type, and is the phone number active.

Collected data is never used for global enrichment of the LexisNexis products. Associations between Login.gov users, devices, email accounts are restricted to GSA staff.

SECTION 5.0 SECURITY

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?

Login.gov employees supporting the LNRS Identity Proofing solution will only have access to information about the transaction that was submitted for verification, but in a limited data capacity. They will have information such as transaction IDs, what checks failed, reason codes, and risk scores. These checks, reason codes and scores do not contain any PII and only provide indications into the nature of the failure or the overall risk score. An example of a reason code would be “The SSN does NOT match the First and Last Name”, but no other information specific to an individual would be provided.

LNRS strives to inform its employees, users and the general public about appropriate use of LNRS products and services, including:

- Privacy and security issues associated with LexisNexis information products and services; and

- The responsible use of personally identifiable information.

Access to the information by Login.gov and LNRS employees is on a need-to-know basis and only for business, legal, or regulatory related requests. Requests for access require manager and program approvals before access can be granted.

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

The initial self-assessment SSP has been documented for GSA Review in accordance with NIST 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.

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

LNRS is working toward the completion of the National Institutes of Standards and Technology (NIST) Special Publication (SP) 800-171, *"Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations"* Third-Party Independent Risk Assessment that will be performed by a certified Third-Party Assessment Organization for all solutions within the Login.gov workflow. All products currently in use have been assessed under Third-Party independent assessments of the Systems and Organizations Controls (SOC 2) and align to the industry standard framework. The True ID product is managed in accordance with the National Institutes of Standards and Technology (NIST) Special Publication (SP) 800-171, *"Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*" and has been certified in compliance with these requirements and has also been assessed by a qualified independent assessor.

The LNRS Information Security program serves to establish security practices for LNRS computer resources and associated communication networks. Access to systems containing sensitive Controlled Unclassified Information (CUI), such as PII is restricted on a need-to-know and business need basis. Login.gov user PII is not retained within the LexisNexis system as outlined above. Multiple security domains are in place to protect the environments and to ensure confidentiality. All data flowing through LNRS infrastructure is encrypted. LNRS scans, identifies, and remediates vulnerabilities in the systems. Security testing requirements are in place to ensure security related functionality is verified frequently. Please see Login.gov PIA at www.gsa.gov/PIA for additional details regarding GSA's continuous monitoring.

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

LNRS has procedures established to protect individuals' privacy through the design of our products, by credentialing, monitoring, and auditing our customers as appropriate, and also through other information security safeguards. LNRS has an internal incident response team that is responsible for establishing all incident response and escalation procedures to ensure timely and effective handling of all situations. All employees are required to complete security and compliance training at the beginning of employment and throughout their tenure with LNRS, and to accept and acknowledge the incident response reporting requirements. As part of LNRS compliance with the National Institutes of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations" all employees supporting the Login.gov identity solution are required to

follow the requirement in reporting security incidents. LNRS will report all incidents impacting or potentially impacting Login.gov to GSA.

Please see Login.gov PIA at www.gsa.gov/PIA for additional details regarding GSA's Incident Response.

If you suspect a potential IT security incident or observe inappropriate use of GSA systems, **report it immediately to ITServiceDesk@gsa.gov or** 866-450-5250

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.

GSA also owns the interface that is collecting the data from the public and must provide any notices required before collection, maintenance, or use of dissemination of personal information. Please see Login.gov Privacy and Security Practices at https://login.gov/policy/ and the GSA Login.gov PIA at www.gsa.gov/PIA for additional details. LexisNexis performs no independent collection, maintenance, use or dissemination of personal information outside of the interface provided by the login.gov interface.

6.2 What procedures allow individuals to access their information?

Login.gov provides access to the personal information it has through their account page. On that account page the user may also choose to delete their information should they desire. Access to information maintained by LNRS is described in Section 6.3.

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

Login.gov does not maintain information about its users within the LNRS product.

LNRS does maintain information about individuals from other sources. This information is used during the proofing process. The LNRS identity solution validates the authenticity of the information and documents submitted by the individuals. Individuals who would like to see the information maintained by LexisNexis can request and receive a copy of their LexisNexis Consumer Disclosure Report by submitting a request to LexisNexis Risk Solutions online. Information disputes can be submitted through the Description of Procedure Letter.

For True ID documentation authentication, LNRS will not accept documentation submitted by the user that does not meet the validation requirements or types of documents that can be used for identity verification. Should that information fail authenticity checks, the user will need to supply new information (i.e., images of their identification document).

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.

All LNRS employees are required to go through security and privacy training when hired, and on an annual basis thereafter. The employee training is configured by role and all roles within the LNRS organization are required to complete security and awareness training. Employees whose role have greater access to data and information have more extensive training assigned due to their access. As part of employment on-boarding, LNRS employees are required to execute confidentiality agreements along with acknowledgment of the RELX Code of Conduct that details protecting data privacy and information. Employees must comply with applicable laws and all company policies relating to protection and use of personal information. Employees must have knowledge of the RELX Information Value Classification Policy, and all company policies related to properly handling personal information. Employees supporting the Login.gov follow a "need to know" access model and only employees that have a business reason would have access to the limited information that is retained related to Login.gov transactions.

SECTION 8.0 ACCOUNTABILITY AND AUDITING

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

LNRS has many safeguards in place to ensure security and compliance on the information that is used in the authentication process. Only employees with a role that has the "need-to-know" are granted access to the limited information that is retained (see section 2.1 for a description of the information retained by LNRS) for support of the Login.gov identity proofing. An automated tool is used to route requests for access to the systems where the Login.gov information is maintained. Manager approval is needed to review the request before access is granted. Employee accesses are audited multiple times a year to ensure access to systems are in accordance with roles, positions, and customer support.

Data retention functionality is in place to ensure only information maintained from the transaction is for product functionality and performance. LNRS prevents the use of data enrichment by utilizing engineered coding that prevents the PII from being stored and added to LNRS public records information. LNRS validates this functionality monthly to ensure compliance with the zero data retention and enrichment requirements. Changes that impact this implementation are reviewed by multiple layers of engineers and management to ensure they are tested prior to implementation.

LNRS reviews the security and compliance of 3rd parties that handle document authentication data on a bi-annual basis. LNRS ensures that 3rd parties do not use submitted data for other purposes, and that such data is not retained or used for enrichment. The 3rd party provides LNRS independent verification evidence every month indicating that these controls are in place and operating properly.

GSA/Login.gov uses the LNRS system for purposes described in Section E of this document. LNRS provides GSA/Login.gov role based access control and auditing capabilities for the limited data maintained. Please see the Login.gov PIA for additional details on their information usage.

Login.gov uses the LNRS system for purposes described in Section E of this document. LNRS provides GSA/Login.gov role based access control and auditing capabilities for the limited data maintained. Please see the Login.gov PIA for additional details on their information usage.

---

[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.