Privacy and Civil Liberties Impact Assessment for the ID.me

November 27, 2023

Reviewing Official

Ryan Law
Deputy Assistant Secretary
Privacy, Transparency, & Records
Departmental Offices
Department of the Treasury

Section 1: Introduction

PCLIAs are required for all systems and projects that collect, maintain, or disseminate personally identifiable information (PII). The system owner completed this assessment pursuant to Section 208 of the E-Government Act of 2002 ("E-Gov Act"), 44 U.S.C. § 3501, Office of the Management and Budget (OMB) Memorandum 03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," and Treasury Directive 25-07, "Privacy and Civil Liberties Impact Assessment (PCLIA)," which requires Treasury Offices and Bureaus to conduct a PCLIA before: (1) developing or procuring information technology (IT) systems or projects that collect, maintain or disseminate PII from or about members of the public, or (2) initiating a new collection of information that: (a) will be collected, maintained, or disseminated using IT; and (b) includes any PII permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons (not including agencies, instrumentalities, or employees of the federal government).

It is the policy of the Department of the Treasury ("Treasury" or "Department") and its Bureaus to conduct a PCLIA when PII is maintained in a system or by a project. This PCLIA provides the following information regarding the system or project: (1) an overview of its purpose and functions; (2) a description of the information collected; (3) a description of the how information is maintained, used, and shared; and (4) an assessment of whether the system or project is in compliance with federal requirements that support information privacy.

Section 2: System Overview

Section 2.1: System/Project Description and Purpose

Treasury's Use of ID.me for Identity Proofing

The Department of the Treasury is using ID.me to satisfy identity proofing standards in order to facilitate the secure exchange of personal and business data with members of the public in furtherance of its mission requirements. ID.me is a Federal Identity, Credential, and Access Management (FICAM) certified[1] cloud provider that hosts an application (also called Software as a Service (SaaS)) that performs identity proofing for government and private sector organizations. ID.me also maintains an identity verification platform that has achieved a Federal Risk and Authorization Management Program (FedRAMP)[2] Moderate Authority to Operate (ATO) for its Identity Gateway.[3] Agencies use SaaS offerings to reduce the use of taxpayer dollars to build redundant government systems to support mission requirements when the same services are already offered in the private sector.

[1] FICAM certification means the cloud provider's technology meets Federal FICAM government requirements, Federal directives, regulations, and certain military and commercial security guidelines.

[2] FedRAMP is a U.S. government-wide program that uses a standardized approach to conducting security assessments, authorization and continuous monitoring for cloud products and services. FedRAMP is a risk-based approach allowing the federal government to securely use cloud services. ID.me achieved FedRAMP Ready status in October 2017.

[3] The ID.me "Gateway" is an identity proofing platform that aligns with NIST 800-63-3 IAL2 and AAL2 requirements (discussed in more detail below).

Authorities Requiring Federal Agency Identity Proofing

Identity crimes, including credit, debit, and other identity theft (including payment card fraud), continue to put information exchanged between the public and federal agencies at risk. In 2014, the White House issued Executive Order (EO) 13681, Improving the Security of Consumer Financial Transactions (3 CFR 13681) to improve the security of consumer financial transactions in both the private and public sectors. Although this EO focused primarily on securing financial transactions online, it also generally required the creation of a process "to help ensure that sensitive data are shared only with the appropriate person or people." To that end, the EO required the development of a process "to ensure that all agencies making personal data accessible to citizens through digital applications require the use of multiple factors of authentication and an effective identity proofing process, as appropriate."

NIST SP 800-63, Digital Identity Guidelines

In 2017, the National Institute for Standards & Technology (NIST) issued SP 800-63, the Digital Identity Guidelines document suite, which included volumes on: (1) Digital Identity Guidelines (Special Publication (SP) 800-63-3); (2) Enrollment and Identity Proofing (SP 800-63A) (covering the process by which subjects/applicants can prove their identities and become enrolled as valid subscribers within an identity system at one of three different levels of risk mitigation [in scenarios where the subject is remote or physically-present during the identity proofing process]); (3) Authentication and Lifecycle Management (SP 800-63B) and (4) Federation and Assertions (SP 800-63C) (collectively, "NIST Identity Guidelines"). The NIST Identity Guidelines provide technical requirements for federal agencies when implementing digital identity services. The guidelines include requirements for identity proofing and user (e.g., employees, contractors, private individuals, and organizations [via designated points of contact]) authentication to support secure interactions and exchanges of information over open networks between users and government IT systems.

OMB Requires Federal Agencies to Follow NIST SP 800-63

In 2019, OMB issued M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management. The memorandum set forth the Federal Government's latest identity, credential, and access management (ICAM) policy and overrode many previous OMB memos on this subject dating back to 2004. This memorandum addresses how federal agencies conduct identity proofing, establish enterprise digital identities, and adopt sound processes for authentication and access control as necessary to maintain information security and privacy. In M-19-17, OMB also required that agencies implement NIST SP 800-63-3 (NIST SP 800-63-3) requirements when conducting identity proofing.

Treasury Enterprise Identity Credential and Access Management (TEICAM)

ICAM consists of the tools, policies and systems that allow an organization to manage, monitor and secure access to protected resources. The Treasury Office of the Chief Information Officer (OCIO) established the Treasury Enterprise Identity Credential and Access Management (TEICAM) Office to design, develop, deploy, manage, and maintain Treasury's ICAM initiatives and offerings. To perform these functions, TEICAM maintains and controls the ICAM hardware and software supporting the Department and its Bureaus in all areas of information and technology, including deploying new services (including, identity assurance/proofing) to Treasury's Offices and Bureaus to enable them to efficiently

utilize technology and align ICAM initiatives and offerings with OMB and NIST policies and requirements.

Identity Assurance and Proofing

Identity assurance is the process by which a user's identity is verified before they are allowed (in certain situations) to interact and exchange information with a federal agency system. The process by which an organization verifies that a subject is who they claim to be is called "identity proofing." Identity is proven using the "verified attributes" of a person or entity (collectively "a subject") outside the organization (in this case, outside Treasury) whose identity requires proofing in order to establish a trusted relationship with the organization. "Verified attributes" are a body of information regarding a person, organization, application, or device engaged in an online transaction.

According to NIST SP 800-63-3, digital authentication is "the process of determining the validity of one or more authenticators used to claim a digital identity." Authentication establishes that a subject attempting to access a digital service (in this case, a Treasury digital service) is in control of the technologies used to authenticate. Successful authentication provides a reasonable risk-based assurance that the subject accessing the service on any given day is the same as the subject that previously accessed the service. In the context of Treasury's use of ID.me, digital identity is authenticated for the purpose of allowing a subject outside the organization to access a Treasury digital service to securely exchange information with a Treasury program.

Privacy/Security Challenges with Digital Identity Proofing

Digital identity proofing is technically challenging from a privacy and security perspective because the process typically involves use of an open network to digitally proof and authenticate subjects. Digital authentication protects privacy by mitigating the risks of unauthorized access to the subject's information. Identity proofing, authentication, and authorization, however, also create privacy risks because they require the processing of the subject's information to prove their identity. These risks and their mitigation will be discussed further below.[4]

Privacy Act Federal Acquisition Regulations (FAR) Included in ID.me Contract

Treasury's Departmental Offices maintains a Blanket Purchase Agreement (BPA) with V3GATE LLC, an ID.me reseller, for Identity Proofing Services ("the Identity Proofing BPA"). Treasury's primary objective in executing the the Identity Proofing BPA was to procure ID.me licenses for TEICAM systems to support the Treasury and its customers. BPAs allow federal agencies to satisfy recurring requirements (i.e., new systems and programs identifying the need for the same product or service already in use by another system or program) and reduce administrative costs by eliminating multiple acquisition efforts.

[4] ID.me also offers In-Person Verification. "Individuals can go to a retail location and prove their identity at a kiosk using government documents, giving them access to a secure credential for important services." https://insights.id.me/face-matching-in-id-me-identity-verification/.

In the Identity Proofing BPA, Treasury included the Federal Acquisition Regulation provisions necessary to cause the requirements of the Privacy Act, Section (m)[5] to be applied the contractor and to subcontractors that operate systems of records. Those requirements will be discussed throughout this PCLIA, where applicable. Treasury will also discuss relevant provisions from the ID.me privacy policy and website[6] where applicable to answer questions in this template.

Other Identity Proofing Options Considered

Treasury considered using the General Services Administration's (GSA) Login.gov application to conduct identity proofing. Login.gov, however, does not currently offer certification complying with NIST's IAL2 standard.[7] Treasury requires IAL2 certification[8] for many of its programs that are currently conducting identity proofing. ID.me offers NIST 800-63-3 Identity Assurance Level 2 and Authenticator Assurance Level 2 accredited credential services.

Treasury Programs Currently Using ID.me Identity Assurance/ Proofing Services

Treasury currently leverages the ID.me solution for the following Treasury programs: the Office Financial Assets Control's (OFAC) Committee on Foreign Investment in the United States (CFIUS) and implementation of various Coronavirus economic relief programs.

- *The CFIUS Case Management System ("CMS") is a secure Web portal hosted by the Department of the Treasury through which parties and counsel/representatives are required to submit declarations and file notices pursuant to 31 C.F.R. part 800 and 31 C.F.R. part 802 (Regulations Pertaining to Certain Investments in the United States by Foreign Persons), and any other*

[5] The Privacy Act of 1974, 5 USC, Section 552a, subsection (m) states that: "When an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system. For purposes of subsection (i) of this section any such contractor and any employee of such contractor, if such contract is agreed to on or after the effective date of this section, shall be considered to be an employee of an agency."

[6] Statements included in this PCLIA from the ID.me privacy policy are provided only to inform the public about ID.me's general policies (policies that control its relationship with its non-Treasury customers). If ID.me's general policies conflict with what is stated in the Treasury BPA for ID.me services, the BPA controls.

[7] On the Login.gov website, it states that: "Login.gov user accounts are either identity proofed or self-asserted. Login.gov continues to work toward achieving certification of compliance with NIST's IAL2 standard from a third-party assessment organization." https://developers.login.gov/attributes/

[8] In SP 800-63A, NIST includes three Identity Assurance Levels (IAL) that describe the information that Credential Service Providers (CSPs) collect, how it is collected

- IAL1: There is no requirement to link the applicant to a specific real-life identity. Any attributes provided in conjunction with the authentication process are self-asserted or should be treated as such (including attributes a Credential Service Provider, or CSP, asserts to an RP).
- IAL2: Evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. IAL2 introduces the need for either remote or physically-present identity proofing. Attributes can be asserted by CSPs to RPs in support of pseudonymous identity with verified attributes.
- IAL3: Physical presence is required for identity proofing. Identifying attributes must be verified by an authorized and trained representative of the CSP. As with IAL2, attributes can be asserted by CSPs to RPs in support of pseudonymous identity with verified attributes.

transaction-related information, to CFIUS. Parties to a transaction (or third persons who have information relevant to a transaction) use ID.me to prove their identity so they can submit declarations to and file notices with CFIUS. CFIUS provides a webpage with instructions for using ID.me.[9]

- *The Treasury Office of Small and Disadvantaged Business Utilization (OSDBU) assists, counsels, and advises small businesses of all types on procedures for contracting with Treasury. The Small Business Electronic Capability Statement (SB e-CS) is an electronic tool that enables companies interested in doing business with Treasury to identify their capabilities for Treasury's acquisition personnel. Small businesses can also schedule counseling sessions with participating Treasury bureaus and Prime vendors. Treasury and its bureaus will be able to search SB e-CS for small businesses' capability statements, review vendors business size and past capabilities, and generate reports. SB e-CS also provides contractual awards to small businesses located in underserved communities to implement Executive Order 13985, "Advancing Racial Equity and Support for Underserved Communities Through the Federal Government," including Historically Black Colleges and Universities & Minority Serving Institutions. SB e-CS uses ID.me to provide small businesses with access to the SB e-CS portal.*[10]
- *Treasury's COVID economic relief programs use ID.me to conduct credentialing and identity proofing to authenticate program recipients seeking benefits, establishing eligibility, and/or fulfilling reporting requirements under the following programs:*
    - *The Coronavirus Aid, Relief, and Economic Security (CARES) Act*[11] *program.*[12]
    - *The Coronavirus Economic Relief for Transportation Services (CERTS) program, which provides eligible transportation service companies with resources to help to maintain payroll, hire back employees who may have been laid off, and cover applicable overhead and operational expenses.*[13]
    - *The Emergency Capital Investment Program (ECIP), established by the Consolidated Appropriations Act of 2021, was created to encourage low- and moderate-income community financial institutions to augment their efforts to support small businesses and consumers in their communities. ECIP participants are required to calculate and provide to Treasury their baseline amount of qualified lending through an Initial Supplemental Report. This baseline is then used to calculate the dividend or interest rates applicable to each participant in accordance with the Rate Reduction Incentive Guidelines and ECIP legal agreements.*[14]
    - *The Small Business Electronic Capability (SBeCS) Portal*

---

[9] The CFIUS instructions for creating an ID.me account can be found at: https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-case-management-system

[10] The Small Business Electronic Capability (SBeCS) Portal instructions for creating an ID.me account can be found at: https://sbecs.treas.gov/IDme_instructions_OSDBU_Portal_03242021.pdf

[11] Also, during the COVID 19 pandemic efforts, when face to face activities were limited and as site closures were identified, the ID me solution provided a temporary solution to onboard Treasury staff virtually for mission critical functions until in person activities were restored.

[12] CFIUS instructions for creating an ID.me account can be found at: https://home.treasury.gov/system/files/136/4112CompliancePortalReg-DetailedInstructions.pdf

[13] Treasury instructions for creating an ID.me account can be found at:. https://home.treasury.gov/policy-issues/coronavirus/assistance-for-american-industry/coronavirus-economic-relief-for-transportation-services

[14] The ECIP Application Portal includes instructions for creating an ID.me account. https://home.treasury.gov/system/files/136/ECIPApplicationPortalRegistration_DetailedInstructions.pdf

This PCLIA covers the use of ID.me for these programs. This PCLIA does not cover IRS's use of ID.me which is covered by a separate IRS PCLIA. SADI CSP - ID.me PCLIA: https://www.irs.gov/pub/irs-pia/id-me-pia.pdf

Other Treasury Bureaus and Offices that require ID.me services in the future may be added to this PCLIA by completing the short form attached in Appendix A. Once completed, approved, and signed, these forms will be included with this PCLIA on the Treasury website where Departmental Offices PCLIAs are posted.[15]

Please check the statement below that applies to your system or project and provide any additional information requested. Please read all possible responses before selecting an answer.

1. ☒ A PCLIA is being done for this system for the first time.
2. ☐ This is an update of a PCLIA previously completed and published under this same system or project name. The date the earlier PCLIA was published was 1.1.2020.
3. ☐ This is an update of a PCLIA previously completed and published for a similar system or project that is undergoing a substantial modification or migration to a new system or project name. The name of that previous PCLIA was [Name the PCLIA here] and the date of its publication was 1.1.2020

Section 2.2: Authority to Collect

Federal agencies must have proper authority before initiating a collection of information. The authority is sometimes granted by a specific statute, by Executive order (EO) of the President or other authority. The following specific authorities authorize the collection of this information:

- *EO 13681, Improving the Security of Consumer Financial Transactions;*
- *44 U.S.C. 3101, Records management by agency heads; general duties;*
- *EO 9397, as amended by EO 13487; and 44 U.S.C. 3534 (collection of Social Security Numbers).*
- *M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management.*

Federal agencies may also collect information pursuant to more general authority. For example, all Treasury systems and projects derive general authority to collect information from:

- *31 U.S.C. 321 – General authorities of the Secretary establish the mission of the Department of the Treasury*
- *5 U.S.C. 301 – Department regulations for the operations of the department, conduct of employees, distribution and performance of its business, the custody, use, and preservation of its records, papers, and property.*

Section 2.2(a): Collection Process

On its website, ID.me maintains a page to answer questions related to its identity proofing services.[16] *On this page, ID.me includes a step-by-step process by which individuals may verify their identity with ID.me. Please see Appendix B for a list of the PII data elements ID.me collects from the ID.me user with their consent, and in conformance with NIST IAL2 requirements. This chart includes ID.me's purpose for collecting each data element or information type. Some of the collection described in the appendix is*

[15] https://home.treasury.gov/footer/privacy-act/privacy-and-civil-liberties-impact-assessments/do-pclia

[16] https://help.id.me/hc/en-us/articles/1500003942181

situational, meaning the information is only collected if certain events occur during the identity proofing process (discussed in more detail in the appendix).

Section 2.3: Privacy Act Applicability; SORN Requirement

Under certain circumstances, federal agencies are allowed to exempt a system of records from certain provisions in the Privacy Act. This means that, with respect to information systems and papers files that maintain records in that system of records, the agency may exempt certain system of records from certain Privacy Act requirements. If this system or project contains records covered by the Privacy Act, the applicable Privacy Act system of records notice(s) (SORNs) (there may be more than one) that cover the records in this system or project must list the exemptions claimed for the system of records (it will typically say: "*Exemptions Claimed for the System*" or words to that effect).

Section 2.3(a) Please check ALL statements below that apply to your system or project and provide any additional information requested. Please read all possible responses before selecting an answer.

1. ☐ The system or project does not retrieve records about an individual using an identifying number, symbol, or other identifying particular assigned to the individual. A SORN is not required with respect to the records in this system.
2. ☒ The system or project does retrieve records about an individual using an identifying number, symbol, or other identifying particular assigned to the individual. A SORN is required with respect to the records in this system.
3. ☐ A SORN was identified in the original PCLIA and a determination was made during this current PCLIA update that modifications [choose one] ☐ were ☐ were not required to that SORN. [If modifications were made, generally describe them here]. The current applicable SORN is: [Provide here the SORN number(s), system of records name(s) and the citation to the SORN(s) in the Federal Register.]
4. ☐ A SORN(s) was not identified or required in the original PCLIA, but a determination was made during this current PCLIA update that a SORN(s) is now required. The applicable SORN(s) is:[Provide here the SORN number(s), system of records name(s) and the citation to the SORN(s) in the Federal Register].
5. ☒ *A SORN was published and no exemptions are taken from any Privacy Act requirements.* ***Treasury .015*** *- General Information Technology Access Account Records - 85 FR 73353 (Nov. 17, 2020). Treasury .015 covers records collected by ID.me for identity proofing and the smaller set of records ID.me transfers to Treasury if individuals are approved by ID.me after completing its identity proofing requirements. This includes: (1) individuals who are authorized to access Treasury information technology resources, including employees, contractors, grantees, fiscal agents, financial agents, interns, detailees, and any lawfully designated representative of the above as well as representatives of federal, state, territorial, tribal, local, international, or foreign government agencies or entities, in furtherance of the Treasury mission; (2) individuals who provide personal information in order to facilitate access to Treasury information technology resources; (3) Industry points-of-contact providing business contact information for conducting business with government agencies; and (4) Individuals who voluntarily join a Treasury-owned and operated web portal for collaboration purposes.*
6. ☐ Exemptions are claimed from the following Privacy Act provisions in the applicable SORN(s): [List here all exemptions taken in the applicable SORN; Hint: it's at the end of the SORN]: The citation to the applicable Notice of Proposed Rulemaking and/or Final Rule is [provide here the Federal Register Citation to the NPRM and Final Rule (if a Final Rule was required)].

Section 3: Information Collection

Section 3.1: Relevant and Necessary

The Privacy Act requires "each agency that maintains a system of records [to] maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President." 5 U.S.C. § 552a (e)(1). It allows federal agencies to exempt records from certain requirements (including the relevant and necessary requirement) under certain conditions. 5 U.S.C. §552a (k). The proposed exemption must be described in a Notice of Proposed Rulemaking ("NPRM"). In the context of the Privacy Act, the purpose of the NPRM is to give the public notice of a Privacy Act exemption claimed for a system of records and solicit public opinion on the proposed exemption. After addressing any public concerns raised in response to the NPRM, the agency must issue a Final Rule. It is possible for some, but not all, of the records maintained in the system or by the project to be exempted from the Privacy Act through the NPRM/Final Rule process.

Section 3.1(a) Exemption Claimed from this Requirement?

1. ☒ *The PII maintained in this system or by this project is **not** exempt from 5 U.S.C. § 552a(e)(1), the Privacy Act's requirement that an agency "maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President." Treasury documented the types of information ID.me requires in order to verify the identity of an ID.me user and also analyzed the PII that ID.me provides to Treasury to implement the identity proofing process results. Treasury determined that the PII ID.me provides to Treasury (discussed in Section 3.2 and Appendix B) as an outcome of the identity proofing process is limited to the PII that is relevant and necessary to perform services required under the Treasury contract for ID.me services contract and once received by Treasury is specifically the information in scope for this provision.*

2. ☐ The PII maintained in this system or by this project ***is*** exempt from 5 U.S.C. § 552a(e)(1), because *[See Appendix B for a list of acceptable bases for claiming this exemption and cut and paste **here** all that apply]*.

Section 3.1(b) Continuously Assessing Relevance and Necessity

1. ☐ The PII in the system is not maintained in a system of records. Therefore, the Privacy requirements do not apply. *[Explain **here** what you do to ensure relevance and necessity despite the fact that the Privacy Act does not apply]*.
2. ☐ The PII in the system is maintained in a system of records, but the agency exempted these records from the relevance and necessity requirement. *[Explain **here** what you do to ensure relevance and necessity to the extent possible despite the fact the records are exempt from this requirement]*.
3. ☐ In conducting the "relevance and necessity" analysis that is documented in this PCLIA, the system owner reevaluated the necessity and relevance of all PII data elements and determined that they are still relevant and necessary. Every time this PCLIA is updated, this ongoing assessment will be revisited. If it is determined at any time that certain PII data elements are no longer relevant or necessary, the system owner will update this PCLIA to discuss how the data element was removed from the system and is no longer collected.

4. ☒ *With respect to the PII ID.me currently collects and maintains in executing work orders against the Identity Proofing BPA and the smaller set of data elements ID.me provides to Treasury if an individual successfully completes the ID.me identity proofing process are limited to only that which is relevant and necessary to perform identity proofing services.*
5. ☒ *With respect to PII maintained in the system or by the project, there is a process in place to continuously reevaluate these processes to ensure the data elements collected by ID.me and the smaller data set transferred to Treasury continue to meet the relevant and necessary standards. During the PCLIA process, the system/program always undergoes a review to ensure the continuing relevance and necessity of the PII collected. When the PCLIA is next reviewed, Treasury will review the data elements ID.me collected and Treasury received from ID.me at the time the PCLIA was last reviewed and the data elements Treasury receives from ID.me at the time of the next (and future) PCLIA reviews to determine if there have been any changes since the last PCLIA review. During these future reviews, Treasury will conduct a relevance and necessity review, with special emphasis placed on any new PII collected by ID.me or Treasury that was not discussed in previous PCLIAs. If necessary (i.e., if not already explained on the ID.me website), Treasury will make inquiries to determine the purpose for ID.me collecting and sharing with Treasury any new data elements. If Treasury determines that particular PII is no longer relevant and necessary in between or during PCLIA updates, this PCLIA will be updated at that time.*

Section 3.2: PII and/or information types or groupings

The information below represents the types of information collected and maintained by ID.me regarding ID.me users that are relevant and necessary to implement the Identity Proofing BPA.

Information individuals provide to ID.me to enroll for identity proofing

According to the ID.me privacy policy,[17] when individuals verify their identity, ID.me collects PII that may include:

- *name,*
- *date of birth,*
- *government issued identification numbers (Social Security, driver's license, passport, passport card, or state ID),*
- *copies of individuals' government issued identification card (e.g., license or passport, passport card, or state ID),*
- *email address,*
- *physical/mailing address,*
- *phone number.*

Information individuals provide to ID.me during interactions with ID.me online and in person.

Individuals who verify their identity with ID.me to conduct business with Treasury may also be asked to provide or may provide voluntarily without prompting:

- *Information individuals provide when corresponding with or providing feedback to ID.me.*
- *Information individuals provide if they visit the ID.me offices (this may include capture of their image during security surveillance, including CCTV).*

Information individuals provide to ID.me automatically during online interactions.

- *Information ID.me collects about individuals (or their network devices) automatically:*

[17] https://www.id.me/privacy

- *when they use ID.me's services (for example, information about the individual's computer or mobile device [including IP address] when they visit ID.me's website)*
- *information about individuals' use of ID.me services and their preferences provided to ID.me;*

Information individuals provide to ID.me automatically via cookies and other technologies.

- *ID.me's website states that it does not use persistent tracking cookies (cookies that track users after they leave the ID.me site). ID.me does use cookies necessary to: operate its website; analyze and improve its website and help individuals find information more easily; and to the extent an ID.me user separately engages other ID.me services (for their own personal purposes) the company may send individuals relevant marketing messages (using the pages on its website that individuals visit and links they open). For more information about ID.me's cookies or other tracking technologies, individuals should visit its ID.me Cookie Policy. On this site, individuals are provided instructions for deleting cookies (including ID.me cookies) based on the browser they use.*
- *ID.me does collect:*
  - *geolocation information, such as information that identifies the approximate location of an individual's device and their IP address, which may be used to estimate their approximate location and to detect and prevent fraud; and*
  - *information collected through device-based tracking technologies, such as cookies, pixels, tags, beacons, scripts, or other technologies.*

- *ID.me collects information about individuals from its trusted contracted vendors, including mobile phone carriers, certain government agencies, licensing bodies, etc.*
- *ID.me may also collect information about individuals from other sources, including but not limited to, authoritative data sources, data licensors, aggregators, or public databases.*

ID.me also collects biometrics as part of some of its services. NIST 800 63-3A Section 5.3.1, discusses verification of strong identity evidence which requires a physical or biometric comparison. To verify individuals in virtual setting, ID.me verifies the identity evidence via biometric comparison.

Information ID.me provides to Treasury

Treasury receives from ID.me a packet of information necessary to verify that an individual provided to ID.me sufficient proof of their identity. That packet of information contains the individual's:

- *name,*
- *date of birth,*
- *home/physical/postal address,*
- *zip code,*
- *personal home phone or cell phone,*
- *full social security number*
- *personal or business email address, and*
- *a universally unique identifier (UUID) created by ID.me for each individual for which it conducts identity proofing.*

3.3 Sources from which PII is obtained

*Focusing on the context in which the data was collected and used (i.e., why it is collected and how it is used), check **ALL** sources from which PII is collected/received and stored in the system or used in the project*

1. ***Members of the Public***

☒ Members of the Public (i.e., including individuals who are current federal employees who are providing the information in their "personal" capacity (unrelated to federal work/employment). All of the following are members of the public. *Please check relevant boxes (based on the context of collection and use in this system) for members of the public whose information is maintained in the system (only check if relevant to the purpose for collecting and using the information):*

☒ Members of the general public (current association with the federal government, if any, is irrelevant to the collection and use of the information by the system or project). PII is collected from members of the general public for identity proofing so they may access a Treasury system.

☐ Retired federal employees. Discuss here how/why PII is collected from this source.

☐ Former Treasury employees. Discuss here how/why PII is collected from this source.

☐ Federal contractors, grantees, interns, detailees etc. Discuss here how/why PII is collected from this source.

☐ Federal job applicants.

☐ Other: [Explain ***here***].

2. ***Current Federal Employees, Interns, and Detailees***

☐ Current Federal employees providing information in their capacity as federal employees (for example, PII collected using OPM or Treasury forms related to employment with the federal government)

☐ Interns. Discuss here how/why PII is collected from this source.

☐ Detailees. Discuss here how/why PII is collected from this source.

☐ Other employment-related positions. [name the position here and discuss how/why PII is collected from this source.].

3. ***Treasury Bureaus (including Departmental Offices)***

☐ Other Treasury Bureaus: (name the bureau(s) here and identify the bureau/office information system from which the PII originated)and (how/why PII is collected from this source.).

4. ***Other Federal Agencies***

☐ Other federal agencies: (name each agency here and explain how/why PII is collected from this source.).

5. ***State and Local Agencies***

☒ State and local agencies: *ID.me collects PII from certain government agencies and licensing bodies.*

6. ***Private Sector***

- ☒ *Private sector organizations: ID.me receives PII from its private sector contracted vendors, which may include but is not limited to, authoritative data sources, data licensors, aggregators, or public databases.*

  Treasury receives certain PII (successful identity proofing results) from ID.me (a private sector organization) (discussed above).

7. ***Other Sources***

   ☐ Other sources not covered above (for example, foreign governments).
   (Name the other sources here and explain how/why PII is collected from this source).

Section 3.3: Privacy and/or civil liberties risks related to collection

When Federal agencies request information from an individual that will be maintained in a system of records, they must inform the individual of the following: "(A) the authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary; (B) the principal purpose or purposes for which the information is intended to be used; (C) the routine uses which may be made of the information, as published pursuant to paragraph (4)(D) of this subsection; and (D) the effects on [the individual], if any, of not providing all or any part of the requested information." 5 U.S.C § 522a(e)(3). This is commonly called a Privacy Act Statement. The OMB Guidelines also note that subsection (e)(3) is applicable to both written and oral (i.e., interview) solicitations of personal information. Therefore, even if a federal employee or contractor has a fixed list of questions that they orally ask the individual in order to collect their information, this requirement applies.

Section 3.3(a) Collection Directly from the Individual to whom the PII pertains

1. ☐ None of the PII in the system was collected directly from an individual to whom it pertains. *[Explain if the third-party/agency from which you obtained the PII actually collected the PII directly from the individuals about whom it pertains. Be prepared to discuss below how you ensure the information received from the third-party is still accurate, complete and timely for the purposes for which you will use it)].* [Explanation here.]
2. *☒ Some or ☐ all of the PII collected by ID.me was collected directly from the individual to whom it pertains. ID.me collects most of the PII necessary to perform identity proofing directly from the individual about whom the information is collected. ID.me also verifies identity using information collected from third-party sources, including ID.me private sector contracted vendors, which may include but is not limited to authoritative data sources, data licensors, aggregators, or public databases. The PII ID.me transmits to Treasury are only those limited data attributes necessary to implement the identity proofing process results pursuant to the Identity Proofing BPA. (See section 3.2). The information used during both the identity verification process conducted by ID.me, as well as that shared with Treasury to implement the identity proofing process, is not collected directly by Treasury from the individual. ID.me collects the information used during verification directly from the user and ID.me's contracted vendors for the purpose of account creation and identity verification / credentialing, and thereafter may share certain limited information, in the form of identity proofing results and related PII, with Treasury to verify that the individual successfully completed the identity proofing process.*

Section 3.3(b) Privacy Act Statements

1. ☐ None of the PII in the system was collected directly from the individuals to whom it pertains. Therefore, a Privacy Act Statement is not required.
2. ☒ Some ☐ All of the PII in the system was collected directly from the individual to whom it pertains. Therefore, a Privacy Act Statement was posted at the point where the PII was collected directly from the individual. That Privacy Act Statement was provided to the individual ☐ on the form in which the PII was collected ☐ on a separate sheet of paper that the individual could retain; or ☐ in an audio recording or verbally at the point where the information was collected (e.g., on the phone) or ☐ other [please explain].
3. The Privacy Act Statement contained the following:
    a. ☒ The authority (whether granted by statute, or by Executive order of the President) which authorizes the solicitation of the information.
    b. ☒ Whether disclosure of such information is mandatory or voluntary.
    c. ☒ The principal purpose or purposes for which the information is intended to be used.
    d. ☒ The individuals or organizations outside of Treasury with whom the information may be/ will be shared.
    e. ☒ The effects on the individual, if any, if they decide not to provide all or any part of the requested information.

Section 3.3(c) Use of Full Social Security Numbers

Treasury is committed to eliminating unnecessary collection, use, and display of full Social Security numbers ("SSN") and redacting, truncating, and anonymizing SSNs in systems and documents to limit their accessibility to individuals who do not have a need to access the full SSN in order to perform their official duties. Moreover, the Privacy Act provides that: "It shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number." Pub. L. No. 93–579, § 7. This provision does not apply to: (1) any disclosure which is required by federal statute; or (2) any disclosure of an SSN to any federal, state, or local agency maintaining a system of records in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual. *Id.* at § 7(a)(2)(A)-(B).

Section 3.3(d) Justification for collecting Social Security Numbers

1. ☐ N/A No full SSNs are maintained in the system or by the project. [*Explain if any portion of the SSN short of the full 9 digits is used in the system: Explain]; if the full SSN is located anywhere in the system (even if it is redacted, truncated or anonymized when viewed by users, please check number 2 below)*].
2. ☒ Full SSNs are maintained in the system or by the project and the following approved Treasury uses of SSNs apply:

    ☐ security background investigations;

    ☐ interfaces with external entities that require the SSN;

    ☐ a legal/statutory basis (e.g. where collection is expressly required by statute);

    ☐ when there is no reasonable, alternative means for meeting business requirements;

    ☐ statistical and other research purposes;

    ☒ *delivery of government benefits, privileges, and services;*

    ☐ for law enforcement and intelligence purposes;

☐ aging systems with technological limitations combined with funding limitations render impracticable system modifications or replacements to add privacy risk reduction tools (partial/truncated/redacted or masked SSNs); and

☒ *as a unique identifier for identity verification purposes.*

NIST 800-63A 8.1.1 notes that "the SSN may achieve identity resolution for Relying Parties (RP), in particular federal agencies that use SSNs to correlate a subscriber to existing records." SSNs are necessary for this reason. According to NIST, an RP is the party "that relies on results of an authentication protocol to establish confidence in the identity or attributes of a subscriber for the purpose of conducting an online transaction." In this case, Treasury is the RP. ID.me uses the SSN to make sure that individuals "are who they say they are." The SSN is requested where necessary to prevent impersonation and deception. The information individuals provide to ID.me is secured and encrypted, and is used only to facilitate verification and prevent fraud.

The interaction between ID.me and Treasury programs/systems requires the use of SSN to reliably identify the user. For this reason, ID.me cannot eliminate the use of SSNs when providing identity proofing and verification services for Treasury. ID.me minimizes the display and transmission of the SSN in any form not required to achieve identity verification.

Section 3.3(e) Controls implemented to limit access to and or improper disclosure of full Social Security Numbers

1. ☐ Full SSNs are ***not*** maintained in the system or by the project.
2. ☒ *Full SSNs **are** collected and maintained by ID.me and the following controls are put in place to reduce the risk that the SSN will be seen or used by someone who does not have a need to use the SSN in order to perform their official duties (check **ALL** that apply):*
    a. ☐ The entire SSN data field is capable of suppression (i.e., being turned off) and the data field is suppressed when the SSN is not required for particular system users to perform their official duties.

    ☐ do not require the SSN to perform their official duties.

    c. ☐ Within the system, an alternative number (e.g., an Employee ID) is displayed to all system users who do not require the SSN to perform their official duties. The SSN is only linked to the alternative number within the system and when reporting outside the system (to an agency that requires the full SSN). The SSN is not visible to system users (other than administrators).

    d. ☐ The SSN is truncated (i.e., shortened to the last 4 digits of the SSN) when displayed to all system users for whom the last four digits (but not the full) SSN are necessary to perform their official duties.

    e. ☐ Full or truncated SSNs are only downloaded to spreadsheets or other documents for sharing within the bureau or agency when disclosed to staff whose official duties require access to the full or truncated SSNs for the particular individuals to whom they pertain. No SSNs (full or truncated) are included in spreadsheets or documents unless required by each recipient to whom it is disclosed in order to perform their official duties (e.g., all recipients have a need to see the SSN for each employee in the spreadsheet).

    f. ☒ *Other: ID.me minimizes the display and transmission of the SSN in any form not required to achieve identity verification.*

Section 3.3(f) Denial of rights, benefits, or privileges for refusing to disclose Social Security Number

1. ☐ N/A No SSNs are maintained in the system or by the project.
2. ☒ To the extent available from the individual seeking to verify their identity with ID.me, the company will collect *full SSNs. No individual will be denied any right, benefit, or privilege provided by law if the individual is not assigned an SSN or refuses to disclose their SSN for use in the system or project. The transfer of full SSN from ID.me to Treasury as part of implementing identity proofing is optional and subject to the discretion of Treasury.*
3. ☐ Full SSNs are collected, and the individual will be denied the following right, benefit, or privilege provided by law if they refuse to disclose their SSN: [please identify the right, benefit, or privilege if the individual will be denied if they choose not to provide their SSN: Identify here]. Denial of this right, benefit or privilege does not violate the law because: [choose one of the two boxes below]:
    a. ☐ SSN disclosure is required by the following Federal statute or Executive Order; **OR**
    b. ☐ The SSN is disclosed to a Federal, state, or local agency that maintains a system of records that was in existence and operating before January 1, 1975, and disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual.

Section 3.3(g) Records describing how individuals exercise First Amendment rights

The Privacy Act requires that Federal agencies "maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity." 5 U.S.C. § 552a(e)(7).

1. ☒ N/A. The system or project does ***not*** maintain information describing how an individual exercises their rights guaranteed by the First Amendment.
2. ☐ The system or project ***does*** maintain information describing how an individual exercises their rights guaranteed by the First Amendment. *If you checked this box, please check the box below that explains Treasury's authorization for collecting this information:*
    a. ☐ The individual about whom the information was collected or maintained expressly authorizes its collection/maintenance. The individual about whom the information was collected or maintained expressly authorized its collection by *[explain here how the individual expressly authorizes collection] (for example, individuals may expressly authorize collection by requesting in writing that Treasury share information with a third party, e.g., their Congressman];*
    b. ☐ The information maintained is pertinent to and within the scope of an authorized law enforcement activity because [generally discuss here the nature and purpose of the information collected and the law enforcement activity];
    c. ☐ The following statute expressly authorizes its collection: [provide here the name of and citation to the statute and the language from that statute that expressly authorizes collection] [*your response MUST contain all three if you use a statute as the basis for the collection*].

Section 4: Maintenance, use, and sharing of the information

Section 4.1: Ensuring accuracy, completeness, and timeliness of information collected, maintained, and shared when it is used to make determinations about individuals

The Privacy Act and Treasury policy require that Treasury bureaus and offices take additional care when collecting and maintaining information about individuals when it will be used to make determinations about those individuals (e.g., whether they will receive a federal benefit). This includes collecting

information directly from the individual where practicable and ensuring that the information is accurate, relevant, timely and complete to assure fairness to the individual when making a determination about them. This section addresses the controls/protections put in place to address these issues.

The Privacy Act requires that Federal agencies "maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination." 5 U.S.C § 552a(e)(5). If a particular system of records meets certain requirements (including the NPRM process defined in Section 3.1 above), an agency may exempt the system of records (or a portion of the records) from this requirement. Exemptions may be found at the bottom of the relevant SORN next to the heading: "*Exemptions Claimed for this System.*"

The primary purpose of the ID.me process is to verify the accuracy, timeliness, and completeness of the data provided by an individual (asserted PII), permitting the user to create a portable identity credential and manage their digital identity across ID.me's entire network. In order to meet the NIST SP 800-63-3 requirements, the system verifies asserted PII against authoritative records. Disclosure of the information necessary to conduct identity proofing is voluntary, so a subject can choose not to provide any of the PII ID.me requires. Subjects may also elect to provide all or only some of the information/PII requested by ID.me during the account creation and/or identity verification process. Subjects may also decide at any time to remove some of the information that they previously provided during identity verification. In addition, an individual can, at any time, opt out of the service entirely, at which point ID.me closes the individual's account and destroys any identity credential associated with the user. If the individual opts out, ID.me will also render all associated PII from the user inactive in ID.me's systems. If the subject chooses not to provide the required information (or elects to abandon the verification process before providing all necessary data elements), the ID.me Identity Gateway application will not be able to verify their identity.

For further information, see the ID.me privacy page.

Section 4.1(a). Exemption from the accuracy, relevance, timeliness, and completeness requirements in section (e)(5) of the Privacy Act

1. ☒ ***None*** *of the information maintained in the system or by the project that is part of a system of records is exempt from the accuracy, relevance, timeliness, and completeness requirements in section (e)(5) of the Privacy Act. With regard to information collected directly by ID.me from service-end-users, the company provides individuals with control over their information included in their account. ID.me users can view their "My Account" portal and see all authorized applications (agencies or organizations to which their credentials were sent), including which specific PII was shared. This allows the individual to identify any inaccurate or stale information in their account that requires update. Individuals can revoke access to their portable ID.me identity credential, and therefore the continued sharing of certain associated personal information, for any authorized application at any time. Individuals may also destroy their ID.me credential at their discretion. Upon destruction of an ID.me identity credential the continued sharing of the associated personal information with all authorized applications ceases.*
2. ☐ All ☐ Some of the PII maintained in the system or by the project is part of a system of records and ***is*** exempt from the accuracy, relevance, timeliness, and completeness requirements in section (e)(5) of the Privacy Act. The exemption claimed for these records is appropriate

because *[please see Appendix B which contains sample justifications for this exemption and provide the appropriate bases **here** [more than one bases may apply]*.

3. ☐ The PII maintained in the system or by the project is ***not***: (a) part of a system of records as defined in section (e)(5) of the Privacy Act; or (b) used to make adverse determinations about individuals (defined in the Privacy Act as U.S. Citizens and legal permanent residents). Instead, the information is used to [*describe how the information is used and why this use does not involve adverse determinations*].
4. ☐ ***None*** of the information maintained in the system or by the project is part of a system of records as defined in section (e)(5) of the Privacy Act, but the information in the system ***is*** used to make adverse determinations about individuals (defined in the Privacy Act as U.S. Citizens and legal permanent residents). Despite the fact that the Privacy Act does not apply, the following protections are in place to ensure fairness to the individual: *explain **here*** .

Section 4.1(b) Protections in place despite exemption from the accuracy, relevance, timeliness, and completeness requirements

1. ☒ ***None*** *of the information maintained in the system or by the project that is part of a system of records is exempt from the accuracy, relevance, timeliness, and completeness requirements in section (e)(5) of the Privacy Act.*
2. ☐ For all information maintained in the system or by the project that is part of a system of records that is exempt from the accuracy, relevance, timeliness, and completeness requirements in section (e)(5) of the Privacy Act, the following efforts are made to ensure accuracy, relevance, timeliness, and completeness to the extent possible without interfering with the (*check one*) ☐ law enforcement ☐ intelligence ☐ other [*describe **here***] mission requirements for which the system or project was created [*choose **ALL** that apply*]:
    a. ☐ The exempt information is ***not*** actually used to make any adverse determinations about individuals.
    b. ☐ The exempt information is ***not*** actually used to make any adverse determinations about individuals without additional research and investigation to ensure accuracy, relevance, timeliness, and completeness.
    c. ☐ Individuals and organizations to whom PII from the system or project is disclosed (as authorized by the Privacy Act) determine its accuracy, relevance, timeliness, and completeness in a manner reasonable for their purposes before they use it to make adverse determinations about individuals.
    d. ☐ Individuals about whom adverse determinations are made using PII from this system or project are given an opportunity to explain or modify their information (*check one*) ☐ before ☐ after the adverse determination is made. During this process, individuals are allowed to: [*discuss **here***
    e. ☐ Other: (*please describe*):

3. ☐ No additional efforts are made to ensure accuracy, relevance, timeliness, and completeness to the extent possible because it would interfere with mission requirements.

Section 4.1(c) Collecting information directly from the individual when using it to make adverse determinations about them.

Section 552a(e)(2) of the Privacy Act requires that Federal agencies that maintain records in a system of records are required to collect information to the greatest extent practicable directly from the individual when the information about them may result in adverse determinations about their rights, benefits, and

privileges under Federal programs. Agencies may exempt a system of records from this requirement under certain circumstances and if certain conditions are met.

ID.me's identity platform provides IAL2 identity proofing for individuals looking to access relevant partner services such as Treasury. In accordance with NIST 800-63A, ID.me, as an approved IAL2 credential service provider, does not determine suitability or entitlement to benefits and services, and instead focuses solely on verifying an applicant's identity for IAL2 proofing and providing that determination to Treasury. ID.me collects information directly from and about an individual to verify their identity. The information is provided by the individual and from contracted vendors which may include but are not limited to, authoritative data sources, data licensors, aggregators, or public databases; the individual seeking to verify their identity has control over the accuracy of the information they provide and is directed to ensure the completeness and accuracy of all information maintained by ID.me. If ID.me finds information inconsistent with the information the individual provides, the individual is given an opportunity to contest ID.me's contrary information/prove the validity of the original information the individual provided, as well as to verify their identity using a different verification channel or method.

Individuals who are unsuccessful in completing ID.me's process may reach out to Treasury to explore alternatives for accomplishing the original intended purpose of their engagement with ID.me.

1. ☒ The records maintained by this system or project are **not** used to make any adverse determinations about individuals.
2. ☐ The records maintained by this system or project may be used to make adverse determinations about individuals with respect to some of the Treasury programs that use …… **and** [check all that apply]

3. ☐ These records ***were*** exempted from the Privacy Act provision that requires collection directly from the subject individual to the greatest extent practicable. Exemption of these records is proper because *[explain here why the records were exempted; sample responses are provided in Appendix B of this template]*.
4. ☐ These records were ***not*** exempted from the requirement to collect information directly from the individual to the greatest extent practicable ***and*** [*check the relevant box below and provide the information requested*].
    ii. ☐ ***All*** records used to make an adverse determination are collected directly from the individual about whom the decision is made.
    ii. ☐ A ***combination*** of records collected from third parties ***and*** directly from the individual about whom the determination is made are used to make the determination because [*please explain **here** why third-party data is required to make this determination; e.g., third-party data is required to verify the accuracy of the information provided by the individual seeking a privilege or benefit].*
    iii. ☐ ***None*** of the records used to make adverse determinations are collected directly from the individual about whom determinations are made because seeking the information directly from the individual might *[select **ALL** that apply]:*

        ☐ alert the individual to the fact that their conduct is being observed or investigated;

        ☐ cause the individual to alter or modify their activities to avoid detection;

        ☐ create risks to witnesses or other third parties if the individual is alerted to the fact that their conduct is being observed or investigated;

☐ Other: *(please describe **here**).*

Section 4.1(d) Additional controls designed to ensure accuracy, completeness, timeliness and fairness to individuals in making adverse determinations

Administrative Controls. Individuals about whom information is collected are given the following opportunities to amend/correct/update their information to ensure it is accurate, timely and complete to the extent reasonably necessary to assure fairness when it is used to make a determination about them:

a. ☒ *ID.me's identity platform provides IAL2 identity proofing for individuals looking to access relevant partner services such as Treasury. In accordance with NIST 800-63A, ID.me as an approved IAL2 credential service provider does not determine suitability or entitlement to benefits and services and instead focuses solely on verifying an applicant's identity for IAL2 proofing and providing information to Treasury about individuals who successfully prove their identity. ID.me collects information directly from and about an individual to verify their identity. The information is provided by the individual and from contracted vendors which may include but are not limited to, authoritative data sources, data licensors, aggregators, or public databases; the individual seeking to verify their identity has control over the accuracy of the information they provide and is directed to ensure the completeness and accuracy of all information maintained by ID.me. The user agrees to the sharing of their information with contracted vendors as part of the ID.me Terms of Service as part of the ID.me registration process. If ID.me finds information inconsistent with the information the individual provides, the individual is given an opportunity to contest ID.me's contrary information/prove the validity of the original information the individual provided, as well as to verify their identity using a different verification channel or method.*

b. ☐ The records maintained in the system or by the project are used to make adverse determinations and (*select one*) ☐ are ☐ are not exempt from the access provisions in the Privacy Act, 5 U.S.C. 552a(d).

c. ☒ Treasury has published regulations in place describing how individuals may seek access to and amendment of their records under the Privacy Act. *The Treasury/bureaus FOIA and Privacy Act disclosure regulations can be found at 31 C.F.R. Part 1, Subtitle A, Subparts A and C. ID.me users may update their information in the ID.me system at any time.*

d. ☐ Individuals who provide their information directly to Treasury for use in the system or by the project are provided notice of the adverse determination and an opportunity to amend/correct/ update their information *[choose one]* ☐ before ☐ after it is used to make a final, adverse determination about them. This is accomplished by [*describe **here** how this process works and the protections in place, including redress/appeals processes; if notice is provided **after** an adverse determination is made, explain **here** why notice could not be provided **before** a determination was made, and the protections in place*]: Descriptions.

e. ☐ Individuals who provide their information directly to Treasury for use in the system or by the project are expressly told at the point where the information is collected that they need to keep their information accurate, current and complete because it could be used to make adverse determinations about them. This is accomplished by [*describe **here** how/where/when individuals are told they need to keep their information updated before it is used to make adverse decisions about them; include the exact language provided to the individuals*]: Description.

f. ☐ All manual PII data entry by federal employees/contractors is verified by a supervisor or other data entry personnel before it is uploaded to the system (e.g., PII entered into the

system from paper records is double-checked by someone else before it's uploaded to the system). This is accomplished by: [describe here how this process works].

g. ☐ Other: [please describe here].

Technical controls. The system or project also includes additional technical controls to ensure that PII is maintained with such accuracy, relevance, timeliness and completeness as is reasonably necessary to assure fairness to the individual when it is used to make a determination about them. The following additional protections are relevant to this system or project

a. ☒ No additional technical controls are available to ensure accuracy, relevance, timeliness and completeness.

b. ☐ Automated data feeds are used to refresh/update the information in the system (where the system is reliant on updates from another system). These automated data feeds occur: [state here the frequency of updates] and [state here what happens when the data is updated and why the system is reliant on another system for its data].

c. ☐ Technical and/or administrative controls are put in place to ensure that when information about an individual is acquired from multiple sources for maintenance in a single file about a particular individual, it all relates to the same individual . This is accomplished by: [describe here the method or process used to ensure that information merged about an individual from multiple sources for inclusion in a single file, all relates to the same person].

d. ☐ Address verification and correction software (software that validates, updates and standardizes the postal addresses in a database).

e. ☐ Other: [please describe here].

Section 4.2 Data-Mining

As required by Section 804 of the Implementing Recommendation of the 9/11 Commission Act of 2007 ("9-11 Commission Act"), Treasury reports annually to Congress on its data mining activities. For a comprehensive overview of Treasury's data mining activities, please review the Department's Annual Privacy Act and Data Mining reports available at: http://www.treasury.gov/privacy/annual-reports.

Section 4.2(a) Is the PII maintained in the system used to conduct data-mining?

1. ☒ The information maintained in this system or by this project ***is not*** used to conduct "data-mining" activities as that term is defined in the 9-11 Commission Act. Therefore, no privacy or civil liberties issues were identified in responding to this question.
2. ☐ The information maintained in this system or by this project ***is*** used to conduct "data-mining" activities as that term is defined in the 9-11 Commission Act. This system is included in Treasury's annual report to Congress which can be found on the external Treasury privacy website.
3. ☐ The information maintained in this system or by this project ***is*** used to conduct "data-mining" activities as that term is defined in the 9-11 Commission Act, but this system is not included in Treasury's annual report to Congress which can be found on the external Treasury privacy website. This system will be added to the next Treasury Data-mining report to Congress.

Section 4.3 Computer Matching

The Computer Matching and Privacy Protection Act (CMPPA) of 1988 amended the Privacy Act by imposing additional requirements when Privacy Act systems of records are used in computer matching programs. Pursuant to the CMPPA, there are two distinct types of matching programs. The first type of matching program involves the computerized comparison of two or more automated federal personnel or payroll systems of records or a system of federal personnel or

payroll records with non-federal records. This type of matching program may be conducted for any purpose. The second type of matching program involves the computerized comparison of two or more automated systems of records or a system of records with non-federal records. The purpose of this type of matching program must be for the purpose of eligibility determinations or compliance requirements for applicants, recipients, beneficiaries, participants, or providers of services for payments or in-kind assistance under federal benefit programs, or recouping payments or delinquent debts under such federal benefit programs. *See* 5 U.S.C. § 522a(a)(8). Matching programs must be conducted pursuant to a matching agreement between the source (the agency providing the records) and recipient agency (the agency that receives and uses the records to make determinations). The matching agreement describes the purpose and procedures of the matching **and** establishes protections for matching records.

Section 4.3(a) Records in the system used in a computer matching program

1. ☐ The PII maintained in the system or by the project ***is not*** part of a Privacy Act system of records.
2. ☒ *The information sent by ID.me to Treasury **is** part of a Privacy Act system of records but **is not** used as part of a matching program*.
3. ☐ The information maintained in the system or by the project ***is*** part of a Privacy Act system of records and ***is*** used as part of a matching program. [If whether a Matching Agreement was executed and published as required by the CMPPA/Privacy Act; if no Matching Agreement was executed, please explain here why]: Explain here.

Section 4.3(b) Is there a matching agreement?

1. ☒ N/A
2. ☐ There is a matching agreement in place that contains the information required by Section (o) of the Privacy Act.
3. ☐ There is a matching agreement in place, but it does not contain all of the information required by Section (o) of the Privacy Act. The following actions are underway to amend the agreement to ensure that it is compliant [discuss **here** the issues that were discovered that required amendment and how those issues are being mitigated/fixed].

Section 4.3(c) What procedures are followed before adverse action is taken against an individual who is the subject of a matching agreement search?

1. ☒ N/A
2. ☐ The bureau or office that owns the system or project conducted an assessment regarding the accuracy of the records that are used in the matching program and the following additional protections were put in place:
   a. ☐ The results of that assessment were independently verified by [*explain how and by whom accuracy is independently verified; include the general activities involved in the verification process*].
   b. ☐ Before any information subject to the matching agreement is used to suspend, terminate, reduce, or make a final denial of any financial assistance or payment under a Federal benefit program to an individual:
      i. ☐ The individual receives notice and an opportunity to contest the findings; **OR**
      ii. ☐ The Data Integrity Board approves the proposed action with respect to the financial assistance or payment in accordance with Section (p) of the Privacy Act before taking adverse action against the individual.

3. ☐ No assessment was made regarding the accuracy of the records that are used in the matching program.

Section 4.4: Information sharing with external (i.e., outside Treasury) organizations and individuals

Section 4.4(a) PII shared with/disclosed to agencies, organizations or individuals outside Treasury

1. ☐ PII maintained in the system or by the project is ***not*** shared with agencies, organizations, or individuals external to Treasury.
2. ☒ PII maintained in the system or by the project **is** shared with the following agencies, organizations, or individuals external to Treasury: *Treasury .015, General Information Technology Access Account Records,*[18] *governs the records ID.me transfers to Treasury to implement Identity Proofing Services. The relevant routine uses in this SORN include disclosures: "F. To contractors and their agents, grantees, experts, consultants, fiscal agent, financial agents, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for Treasury, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to Treasury officers and employees" and "[t]o sponsors, employers, contractors, facility operators, grantees, experts, fiscal agents, financial agents, and consultants in connection with establishing an access account for an individual or maintaining appropriate points of contact and when necessary to accomplish a Treasury mission function or objective related to this system of records."*

   *Furthermore, ID.me provides all individuals who register for its identity proofing services (whether federal government or private sector customers) control of their personal information (including to whom it is disclosed). . Before providing information to an organization, ID.me presents a consent screen to the user. The user must provide consent in order for ID.me to release their information to the Relying Party (the organization seeking to verify the individual's identity). ID.me Privacy Statement ("**You** are solely in control of your own Personal Information. **You** must provide consent before we will share any of your Personal Information.")*[19] *This statement means that ID.me only conducts identity proofing and sends the results to an agency or organization if the individual makes such a request." If the individual does not consent (declines), no information is released to the organization (in this case, Treasury). Individuals may also revoke access to the Relying Party (i.e., Treasury) for current (before the information is sent) or future transactions. Individuals only need to send an email to help@ID.me, submit an ID.me support ticket, or revoke consent themselves in the My Account portal.*

   The ID.me privacy policy notifies individuals that ID.me shares data with particular third parties in order to verify information the individual provides to ID.me.

   Moreover, according to its Privacy Statement, ID.me does not sell, rent, or trade any of the PII individuals provide during its identity verification processes.

[18] https://www.federalregister.gov/documents/2016/11/07/2016-26662/privacy-act-of-1974-systems-of-records

[19] https://www.id.me/privacy

3. ☐ All external disclosures ***are*** authorized by the Privacy Act (including routine uses in the applicable SORN).

Section 4.4(b) Accounting of Disclosures

An accounting of disclosures is a log of all external (outside Treasury) disclosures of records made from a system of records that has ***not*** been exempted from this accounting requirement. This log must either be maintained regularly or be capable of assembly in a reasonable amount of time after an individual makes a request. Certain system of records may be exempted from releasing an accounting of disclosures (e.g., in law enforcement investigations). *Check toward the bottom of the SORN to see whether an exemption was claimed from 5 U.S.C. 552a(c). The NPRM and/or Final Rule for the system of records will explain why that exemption is appropriate. ID.me users may see all disclosures they approved within their account in the ID.me system at any time.*

Section 4.4(c) Making the Accounting of Disclosures Available

1. ☐ The records are not maintained in a system of records subject to the Privacy Act so an accounting is ***not*** required.
2. ☐ No external disclosures are made from the system.
3. ☐ The Privacy Act system of records maintained in the system or by the project ***is*** exempt from the requirement to make the accounting available to the individual named in the record. Exemption from this requirement was claimed because: [please state here why the records in this system of records were exempted from this requirement].
4. ☒ *The Privacy Act system of records maintained in the system or by the project is **not** exempt from the requirement to make the accounting available to the individual named in the record and a log is maintained regularly. The log is maintained for at least five years and includes the date, nature, and purpose of each disclosure (not including intra-agency disclosures and FOIA disclosures) of a record to any person or to another agency (outside of Treasury) and the name and address of the person or agency to whom the disclosure is made. The information Treasury receives from ID.me and stores is in scope for conformance with these disclosure requirements. The individual can see all external disclosures they previously approved by logging into their ID.me account.*
5. ☐ The Privacy Act system of records maintained in the system or by the project is ***not*** exempt from the requirement to make the accounting available to the individual named in the record and a log is ***not*** maintained regularly but is capable of being constructed in a reasonable amount of time upon request. The information necessary to reconstruct the log (i.e., date, nature, and purpose of each disclosure) is maintained for at least five years.

Section 4.4(d) Obtaining Consent Prior to New Disclosures Not Authorized by the Privacy Act

Records in a system of records subject to the Privacy Act may not be disclosed by "any means of communication to any person or to another agency" without the prior written request or consent of the individuals to whom the records pertain. 5 U.S.C. Sec. 552a(b). However, the Act also sets forth twelve exceptions to this general restriction. These 12 exceptions may be viewed at: https://www.justice.gov/usam/eousa-resource-manual-139-routine-uses-and-exemptions. Unless one of these 12 exceptions applies, the individual to whom a record pertains must provide their consent, where feasible and appropriate, before their records may be disclosed to anyone who is not listed in one of the 12 exceptions. One of these 12 exceptions also allows agencies to include in a notice published in the Federal Register, a list of routine

uses. Routines uses are disclosures outside the agency that are compatible with the purpose for which the records were collected.

Section 4.4(e) Obtaining Prior Written Consent

1. ☐ The records maintained in the system of records are only shared in a manner consistent with one of the 12 exceptions in the Privacy Act, including the routine uses published in the Federal Register.
2. ☐ If a situation arises where disclosure (written, oral, electronic, or mechanical) must be made to anyone outside of Treasury who is not listed in one of the 12 exceptions in the Privacy Act (including the published routine uses), the individual's prior written consent will be obtained where feasible and appropriate.
3. ☒ *Other: The individual has complete control over the organizations to which ID.me discloses a subset of the information they provide to ID.me for identity verification purposes.*

Section 5: Compliance with federal information management requirements

Responses to the questions below address the practical, policy, and legal consequences of failing to comply with one or more of the following federal information management requirements (to the extent required) and how those risks were or are being mitigated: (1) the Privacy Act System of Records Notice Requirement; (2) the Paperwork Reduction Act; (3) the Federal Records Act; (4) the E-Gov Act security requirements; and (5) Section 508 of the Rehabilitation Act of 1973.

Section 5.1: The Paperwork Reduction Act

The PRA requires OMB approval before a Federal agency may collect standardized data from 10 or more respondents within a 12-month period. OMB also requires agencies to conduct a PIA (a Treasury PCLIA) when initiating, consistent with the PRA, a new electronic collection of PII for 10 or more persons (excluding agencies, instrumentalities, or employees of the federal government).

Section 5.1(a).

☐ The system or project maintains information obtained from individuals and organizations who are not federal personnel or an agency of the federal government (i.e., outside the federal government).

2. ☐The project or system involves a new collection of information in identifiable form for 10 or more persons from outside the federal government.
3. ☐ The project or system completed an Information Collection Request ("ICR") and received OMB approval.
4. ☒ The project or system did not complete an Information Collection Request ("ICR") and receive OMB approval because ID.me only requests information necessary to identify the individual, which falls within an exemption to the law.

Section 5.2: Records Management - NARA/Federal Records Act Requirements

Records retention schedules determine the maximum amount of time necessary to retain information in order to meet the needs of the project or system. Information is generally either disposed of or sent to the National Archives and Records Administration (NARA) for permanent retention upon expiration of this

period. If the system has an applicable SORN(s), check the "Policies and Practices for Retention and Disposal of Records" section.

Section 5.2(a)

1. ☒ *The records used in the system or by the project are covered by a NARA's General Records Schedule (GRS). As a certified identity provider, ID.me is required to store the individual's attributes in order to make the digital identity interoperable at a high level of assurance. I*
    - *GRS 3.2 Item 060/061-PKI administrative records Federal Bridge Certification Authority Certification Authority (FBCA CAs). Destroy/delete when 7 years 6 months, 10 years 6 months, or 20 years 6 months old, based on the maximum level of operation of the CA, or when no longer needed for business, whichever is later.*

- *GRS 5.6 Item 120-Personal identification credentials and cards-Application and activation records-Destroy mandatory and optional data elements housed in the agency identity management system and printed on the identification card 6 years after terminating an employee or contractor's employment, but longer retention is authorized if required for business use.*

2. ☐ The records used in the system or by the project are covered by a NARA approved Treasury bureau Specific Records Schedule (SRS). The SRS *[please provide here the specific schedule name and identifying number]*
3. ☐ On [*please state the date on which NARA approval was sought*] the system owner sought approval from NARA for an SRS and is awaiting a response from NARA. *[State here the retention periods you proposed to NARA]*.
4. ☐ The system owner is still in the process of developing a new records schedule to submit to NARA.

Section 5.3: E-Government Act/NIST Compliance

The completion of Federal Information Security Management Act (FISMA) Security Assessment & Authorization (SA&A) process is required before a federal information system may receive Authority to Operate (ATO).

Section 5.3(a)

1. ☒ *ID.me is a certified identity verification platform that has achieved a Federal Risk and Authorization Management Program (FedRAMP) Moderate Authority to Operate (ATO) for its Identity Gateway.*[20] *ID.me also adheres to the requirements outlined in the NIST SP 800-63-3. ID.me offers:*
    a. *ID.me uses multi-factor authentication (MFA) to confirm an individual's identity when they sign in to their ID.me account. MFA strengthens account security by requiring two factors to confirm identity. This usually includes something the individual knows (like a username and password) plus something the individual owns (like a phone number). ID.me offers a variety of options for MFA. ID.me*

[20] FedRAMP is a U.S. government-wide program that uses a standardized approach to conducting security assessments, authorization and continuous monitoring for cloud products and services. FedRAMP is an effective, risk-based approach for the adoption and use of cloud services by the federal government. ID.me achieved FedRAMP Ready status in October 2017 and, with sponsorship from the United States Department of Veterans Affairs (VA), has received its ATO and is now available in the FedRAMP Marketplace for other federal agencies to use.

also employs role-based access controls (RBAC) to servers containing PII. Authorization is done on a least privilege model with access changes requiring ticket and management approval. ID.me personnel are required to complete annual security awareness and privacy training.

b. *All information individuals provide to ID.me is encrypted and secured in transit and at rest.*

2. ☐ The system is a federal information system subject to FISMA requirements.
3. ☐ The system last completed an SA&A and received an ATO on: [*state the date when the system was last authorized to operate by an Authorizing Official*].
4. ☐ This is a new system has not yet been authorized to operate. The expected to date for receiving ATO is *[please state here the expected date on which you expect authorization will be granted]*.
5. ☐The system or project maintains access controls to ensure that access to PII maintained is limited to individuals who have a need to know the information in order to perform their official Treasury duties.
6. ☐ All Treasury/bureau security requirements are met when disclosing and transferring information (e.g., bulk transfer, direct access by recipient, portable disk, paper) from the Treasury system or project to internal or external parties.
7. ☐ This system or project maintains an audit log of system users to ensure they do not violate the system and/or Treasury/bureau rules of behavior.
8. ☐ This system or project has the capability to identify, locate, and monitor individuals or groups of people other than the monitoring of system users to ensure that they do not violate the system's rules of behavior. *[If checked, please describe this capability here, including safeguards put in place to ensure the protection of privacy and civil liberties.]*

Section 5.4: Section 508 of the Rehabilitation Act of 1973

When Federal agencies develop, procure, maintain, or use Electronic and Information Technology (EIT), Section 508 of the Rehabilitation Act of 1973 (as amended in 1998) requires that individuals with disabilities (including federal employees) must have access and use (including privacy policies and directives as well as redress opportunities) that is comparable to that which is available to individuals who do not have disabilities.

Section 5.4(a)

1. ☐ The project or system will ***not*** involve the development, procurement, maintenance or use of EIT as that term is defined in Section 508 of the Rehabilitation Act of 1973 (as amended in 1998)?
2. ☒ The project or system ***will*** involve the development, procurement, maintenance or use of EIT as that term is defined in Section 508 of the Rehabilitation Act of 1973 (as amended in 1998)? *If checked:*
3. ☒ The system or project complies with all Section 508 requirements, thus ensuring that individuals with disabilities (including federal employees) have access and use (including access to privacy and civil liberties policies) that is comparable to that which is available to individuals who do not have disabilities.
4. ☐ The system or project is not in compliance with all Section 508 requirements. The following actions are in progress to ensure compliance: [please describe here the efforts underway to ensure compliance*]*.

Responsible Officials
Approval Signature

_____

Ryan Law
Deputy Assistant Secretary
Privacy, Transparency, & Records

Appendix A

Additional Treasury Uses of ID.me Incorporated by Reference Into this PCLIA

In this appendix Treasury identifies additional programs/systems that are using ID.me (after the date the ID.me Privacy and Civil Liberties Impact Assessment (PCLIA) was signed). By completing the form in this appendix, the program/system is incorporated by reference into the ID.me PCLIA. The programs and systems referenced below all maintain a separate PCLIA ("the program/system PCLIA") for other (non-ID.me) information collected when executing mission requirements. These additional programs/systems will cross-reference this ID.me PCLIA in the program/system PCLIA.

Name of Treasury Bureau/Office using ID.me:

Name of the program/system PCLIA and link to its location:

Description of the program/system and how it uses ID.me (*including IAL level***):**

Description of any of the program's/system's ID.me collection, use, maintenance, and disclosure issues that differ from the sections in the ID.me PCLIA: [*describe differences here or state "There are no differences."*]

Program/System Manager: I am the individual responsible for this program/system. I have reviewed the ID.me PCLIA and described above all of my program's/system's collection, use, maintenance, and disclosure issues that differ from that document, if any.

_____
Program/System Manager Signature

_____
Privacy, Transparency, & Records Signature

Appendix B

Chart of Information ID.me collects for identity proofing at Treasury and the purpose for its collection

PII ID.me collects from Treasury customers	
Data Element	**Purpose of collection**
Personal or business email address	Account setup (to establish control of the account; to send a code to confirm with the owner of the email account provided that the account was used to establish an ID.me account; to receive information from ID.me about in person appointments)
Physical home/mailing address (provided in driver's license and other identification verification documents)	Account setup/enrollment
Post Office (P.O.) Box	Account setup (if driver's license lists P.O. Box as home address)
Username and password (for the ID.me site)	One of the factors used as part of multi-factor authentication
Phone number	Identity verification and one of the factors used as part of multi-factor authentication. The use of mobile phones is required in order for the applicant to complete the IAL2 identity proofing process. Mobile phones are used as a piece of identity evidence themselves and to capture additional identity evidence (e.g., photo of government issued identification document). Geolocation can be collected from the Mobile Network Operators (MNOs) in the event of an investigation into a user
Photograph (optional)	Identity verification (compare to information in photo ID provided during account setup)
Selfie Image	Identity verification (to confirm liveness of the individual depicted in photo ID provided earlier)
Video (interaction online during video call with ID.me trusted referee)	Identity verification and to provide customer services related to ID.me products
Driver's License, Passport, Passport Card, or State ID information (including photograph)	Identity verification (to compare with information in photo ID provided earlier during enrollment)
Biometric data	Identity verification (required as part of some of ID.me's services)
Social Security Number	Identity verification (to prevent duplication, impersonation, and deception via use of a unique identifier)
Date of birth	Identity verification (comparison with information in documentation provided)
● Images of STRONG and / or FAIR evidence types	Identity verification, to perform its contracts with/provide its services to individuals and organizations. List of accepted documents can be found here.
● Information ID.me collects about individuals (or their network devices) automatically: o when they use ID.me's services (for example, information about the individual's computer or mobile device when they visit ID.me's website) o geolocation information, such as information that identifies the approximate location of an individual's device and their IP address, which may	To maintain the safety and security of [its] services, to protect "the rights and property of ID.me and others, and to comply with legal obligations including to detect, investigate, and prevent fraud and other illegal activities and to enforce [its] agreements."

be used to estimate their approximate location; and	
○ information about individuals' use of ID.me services and their preferences provided to ID.me; ○ information collected through device-based tracking technologies, such as cookies, pixels, tags, beacons, scripts, or other technologies. ● Information collected using cookies to collect information regarding the pages on its website that individuals visit and links they open.	To analyze uses and improve its website and help individuals find information more easily. The PII for individuals using ID.me services in connection with legal identity verification for a state or federal government agency are not used for any type of marketing or promotional purposes. Other users (not associated with state and federal verification) may opt in to ID.me marketing messages, promotional messages (including for the ID.me Shop), products or services that might be of interest.
● ID.me verifies the identity using information collected from third-party sources, including ID.me contracted vendors, which may include but is not limited to authoritative data sources, data licensors, aggregators, or public databases.	To verify the accuracy of the information the individual provides during verification with ID.me.
PII Treasury receives back from ID.me	
● name, ● middle name, ● last name, ● date of birth, ● street, ● city, ● state,, ● zip code, ● personal home phone or cell phone, ● full social security number ● personal or business email address, and ● a universally unique identifier (UUID) created by ID.me for each individual for which it conducts identity proofing.	To complete the Identity Proofing/Verification process so it can exchange information with the individual (and/or the organization for which the individual is a point of contact).