



## **Litigation Support System**

**PRIVACY AND CIVIL LIBERTIES IMPACT ASSESSMENT (PCLIA)**  
Publication Date: March 8, 2022

**Reviewing Official**

**Ron Shelden, Privacy Program Manager**

---

**OFFICE OF THE COMPTROLLER OF THE CURRENCY**

## Risk Level

Please check **ALL** that apply to the information system or information technology (IT) for which you are conducting this PCLIA:

- This PCLIA is for a “major information system”
- This PCLIA is for an information system or IT rated “Moderate” or “High” impact for confidentiality under Federal Information Processing Standard 199, at least in part because of its PII content.
- This PCLIA is for an information system or IT designated as a Treasury High Value Asset (HVA).

## Estimated number of individuals whose PII is maintained in the system

- |  |   |  |
|--|---|--|
| <input type="checkbox"/> 0 – 999           | <input checked="" type="checkbox"/> 1,000 – 9,999 | <input type="checkbox"/> 10,000 – 99,999 |
| <input type="checkbox"/> 100,000 – 499,999 | <input type="checkbox"/> 500,000 – 999,999        | <input type="checkbox"/> 1,000,000+      |

## Section 1: Introduction

This PCLIA provides the following information regarding the system:

- (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;
- (4) an assessment of whether the system is in compliance with federal requirements that support information privacy; and
- (5) an overview of the redress/complaint procedures available to individuals who may be affected by the use or sharing of information by the system.

## Section 2: System Overview

### **Section 2.1:**

#### **System Description**

LSS replaced legacy and on-premise versions of litigation support applications, SummationPro and eCapture. LSS collects and maintains information used to conduct investigations into individuals or financial institutions as part of OCC litigation cases.

#### **System Purpose**

Litigation Support System (LSS) is used by the Chief Counsel Office (CCO) to provide eDiscovery and electronic evidence processing to support OCC legal matters.

## 2.1. Is this a new information system or a significant revision of an existing system?

- New system
- Revision of Existing system.
- No significant change in existing system

## Section 2.2: Authority to Collect

12 U.S.C. §§ 1, 93(d) (second), 481, 1818, and 1820

Section 93(d) of 12 USC states:

Authority: The Comptroller of the Currency may act in the Comptroller's own name and through the Comptroller's own attorneys in enforcing any provision of title 62 of the Revised Statutes, regulations thereunder, or any other law or regulation, or in any action, suit, or proceeding to which the Comptroller of the Currency is a party.

## Section 2.3: Privacy Act Applicability; SORN Requirement

### Section 2.3(a) Please check ALL statements below that apply to your system and provide any additional information requested.

1.  The system 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 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  were  were not required to that SORN. The current applicable SORN is: 81 FR 2945, 2956-7. (2016). Treasury CC.510 covers the category of individuals and the types of records in LSS.
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.
5.  A SORN was published and no exemptions are taken from any Privacy Act requirements.
6.  Exemptions are claimed from the following Privacy Act provisions in the applicable SORN(s):

## Section 3: Information Collection

## Section 3.1: Relevant and Necessary

### Section 3.1(a) Exemption Claimed from this Requirement?

- 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.*"
- The PII maintained in this system or by this project **is** exempt from 5 U.S.C. § 552a(e)(1), because 5 U.S.C. § 552a(j)(2) and 5 U.S.C. § 552a(k)(2) permit the exemptions to the provisions (see 31 CFR 1.36 - <https://www.govinfo.gov/content/pkg/CFR-2018-title31-voll/xml/CFR-2018-title31-voll-sec1-36.xml>).

### Section 3.1(b) Continuously Assessing Relevance and Necessity

- The PII in the system is not maintained in a system of records. Therefore, the Privacy requirements do not apply.
- The PII in the system is maintained in a system of records, but the agency exempted these records from the relevance and necessity requirement. PII maintained in system is used for investigations and litigation and is not subject to Privacy Act's relevant and necessary requirement. Exemption under 5 USC 552a(c)(3); 5 USC 522a(d)(1), (2), (3), and (4); 5 USC 552a(e)(1), (e)(4)(G), (H), and (I); 5 USC 552a(f) as identified in 66 FR 54175-01, 2001 WL 1294561 (F.R.) Notice of Proposed Rulemaking (NPRM). As noted in the NPRM, there are a number of reasons for exemption, including that the application of the relevant and necessary requirement could impair the OCC's ability to collect, utilize and disseminate valuable law enforcement information. For example, in many cases, especially in the early stages of investigation, it may be impossible immediately to determine whether information collected is relevant and necessary, and information that initially appears irrelevant and unnecessary often may, upon further evaluation or upon collation with information developed subsequently, prove particularly relevant.
- The system owner conducted an assessment prior to collecting PII for use in the system.
- With respect to PII **currently** maintained (as of the time this PCLIA is being done) in the system, the PII  is  is not limited to only that which is relevant and necessary to meet the system's or project's mission requirements. During the PCLIA process, the system always undergoes a review to ensure the continuing relevance and necessity of the PII in the system.
- With respect to PII maintained in the system, there  is  is not a process in place to continuously reevaluate and ensure that the PII remains relevant and necessary. During the PCLIA process, the system always undergoes a review to ensure the continuing relevance and necessity of the PII on the system. If a determination is made that particular PII is no longer relevant and necessary in between PCLIA updates, this PCLIA will be updated at that time.

## Section 3.2: PII and/or information types or groupings

### Biographical/general information

- |  |   |  |
|--|---|--|
| <input checked="" type="checkbox"/> Name   | <input checked="" type="checkbox"/> Nationality                 | <input checked="" type="checkbox"/> Country of Birth             |
| <input checked="" type="checkbox"/> Age  | <input checked="" type="checkbox"/> Citizenship                 | <input checked="" type="checkbox"/> Immigration Status           |
| <input checked="" type="checkbox"/> Date of birth                                  | <input checked="" type="checkbox"/> Ethnicity                   | <input checked="" type="checkbox"/> Alias (including nickname)   |
| <input checked="" type="checkbox"/> Home physical/postal mailing address           | <input checked="" type="checkbox"/> Gender                      | <input checked="" type="checkbox"/> City or County of Birth      |
| <input checked="" type="checkbox"/> Zip Code                                       | <input checked="" type="checkbox"/> Race                        | <input checked="" type="checkbox"/> Military Service Information |
| <input checked="" type="checkbox"/> Personal home phone, cell phone, or fax number | <input checked="" type="checkbox"/> Personal e-mail address     | <input checked="" type="checkbox"/> Country or city of residence |
|  | <input checked="" type="checkbox"/> Other: Mother's Maiden Name |  |

### Other information

- |   |   |  |
|---|---|--|
| <input checked="" type="checkbox"/> Resume or curriculum vitae  | <input checked="" type="checkbox"/> Cubical or office number  | <input checked="" type="checkbox"/> Veteran's preference               |
| <input checked="" type="checkbox"/> Religion/Religious Preference   | <input checked="" type="checkbox"/> Education Information (proof and status of education)                     | <input checked="" type="checkbox"/> Spouse Information                 |
| <input checked="" type="checkbox"/> Professional/personal references or other information about an individual's friends, associates or acquaintances. | <input type="checkbox"/> Contact lists and directories (known to contain at least some personal information). | <input checked="" type="checkbox"/> Retirement eligibility information |
| <input checked="" type="checkbox"/> Sexual Orientation  | <input checked="" type="checkbox"/> Marital Status  | <input checked="" type="checkbox"/> Information about other relatives. |
| <input checked="" type="checkbox"/> Group/Organization Membership   | <input checked="" type="checkbox"/> Information about children  | <input type="checkbox"/> Other:  |

### Identifying numbers assigned to individuals

- |  |   |  |
|--|---|--|
| <input checked="" type="checkbox"/> Full Social Security number                            | <input checked="" type="checkbox"/> Personal device identifiers or serial numbers | <input checked="" type="checkbox"/> Vehicle Identification Number  |
| <input checked="" type="checkbox"/> Truncated Social Security Number (e.g., last 4 digits) | <input checked="" type="checkbox"/> Internet Protocol (IP) Address                | <input checked="" type="checkbox"/> Driver's License Number  |
| <input checked="" type="checkbox"/> Employee Identification Number                         | <input checked="" type="checkbox"/> Personal Bank Account Number                  | <input checked="" type="checkbox"/> License Plate Number   |
| <input checked="" type="checkbox"/> Taxpayer Identification Number                         | <input checked="" type="checkbox"/> Health Plan Beneficiary Number                | <input checked="" type="checkbox"/> Professional License Number  |
| <input checked="" type="checkbox"/> File/Case ID Number                                    | <input checked="" type="checkbox"/> Credit Card Number                            | <input checked="" type="checkbox"/> Passport Number and information (full name, passport number, DOB, POB, sex, nationality, photograph, signature, date and place of issuance, and expiration date) |
| <input checked="" type="checkbox"/> Alien Registration Number                              | <input checked="" type="checkbox"/> Patient ID Number                             | <input type="checkbox"/> Other:  |

### Specific Information/File Types

- |   |   |   |
|---|---|---|
| <input checked="" type="checkbox"/> Taxpayer Information/Tax Return Information   | <input checked="" type="checkbox"/> Law Enforcement Information   | <input checked="" type="checkbox"/> Security Clearance/Background Check Information                         |
| <input checked="" type="checkbox"/> Civil/Criminal History Information/Police Records (obtained from government source)   | <input checked="" type="checkbox"/> Civil/Criminal History Information/Police Records (obtained from commercial source) | <input type="checkbox"/> Credit History Information (government source)                                     |
| <input type="checkbox"/> Protected Information (as defined in Treasury Directive 25-10)   | <input checked="" type="checkbox"/> Credit History Information (commercial source)                                      | <input checked="" type="checkbox"/> Bank Secrecy Act Information  |
| <input checked="" type="checkbox"/> Information provided under a confidentiality agreement  | <input checked="" type="checkbox"/> Case files  | <input checked="" type="checkbox"/> Personnel Files   |
| <input checked="" type="checkbox"/> Business Financial Information (including loan information)   | <input checked="" type="checkbox"/> Personal Financial Information (e.g., loan information)                             | <input checked="" type="checkbox"/> Information subject to the terms of an international or other agreement |
| <input checked="" type="checkbox"/> Passport information (full name, passport number, DOB, POB, sex, nationality, photograph, signature, date and place of issuance, and expiration date) | <input type="checkbox"/> Other:   |   |

### Audit Log and Security Monitoring Information

- |  |   |  |
|--|---|--|
| <input type="checkbox"/> User ID assigned to or generated by a user of Treasury IT             | <input type="checkbox"/> Files and folders accessed by a user of Treasury IT                                    | <input type="checkbox"/> Biometric information used to access Treasury facilities or IT  |
| <input type="checkbox"/> Passwords generated by or assigned to a user of Treasury IT           | <input type="checkbox"/> Internet or other queries run by a user of Treasury IT                                 | <input type="checkbox"/> Contents of files accessed by a user of Treasury IT   |
| <input type="checkbox"/> Files accessed by a user of Treasury IT (e.g., web navigation habits) | <input checked="" type="checkbox"/> Date and time an individual accesses a facility, system, or other IT        | <input checked="" type="checkbox"/> Information revealing an individual's presence in a particular location as derived from security token/key fob, employee identification card scanners or other IT. |
| <input type="checkbox"/> Public Key Information (PKI).   | <input checked="" type="checkbox"/> Still photos of individuals derived from security cameras.                  | <input type="checkbox"/> Purchasing habits or preferences  |
| <input checked="" type="checkbox"/> Internet Protocol (IP) Address                             | <input checked="" type="checkbox"/> Video of individuals derived from security cameras                          | <input checked="" type="checkbox"/> Commercially obtained internet navigation/purchasing habits of individuals   |
| <input type="checkbox"/> Global Positioning System (GPS)/Location Data                         | <input checked="" type="checkbox"/> Secure Digital (SD) Card or Other Data stored on a card or other technology | <input type="checkbox"/> Device settings or preferences (e.g., security level, sharing options, ringtones).  |
| <input type="checkbox"/> Network communications data   | <input type="checkbox"/> Cell tower records (e.g., logs. user location, time etc.)                              | <input checked="" type="checkbox"/> Other: Usernames, avatars etc.   |

### Medical/Emergency Information Regarding Individuals

- |  |  |   |
|--|--|---|
| <input checked="" type="checkbox"/> Medical/Health Information | <input checked="" type="checkbox"/> Worker's Compensation Act Information                                  | <input checked="" type="checkbox"/> Emergency Contact Information (e.g., a third party to contact in case of emergency) |
| <input checked="" type="checkbox"/> Mental Health Information  | <input checked="" type="checkbox"/> Information regarding a disability                                     | <input checked="" type="checkbox"/> Patient ID Number   |
| <input checked="" type="checkbox"/> Sick leave information     | <input checked="" type="checkbox"/> Request for an accommodation under the Americans with Disabilities Act | <input type="checkbox"/> Other:   |

### Biometrics/Distinguishing Features/Characteristics of Individuals

- |  |  |   |
|--|--|---|
| <input checked="" type="checkbox"/> Physical description/ characteristics (hair, eye color, weight, height, sex, gender, etc.) | <input checked="" type="checkbox"/> Signatures       | <input type="checkbox"/> Palm prints                      |
| <input type="checkbox"/> Fingerprints  | <input checked="" type="checkbox"/> Photos and Video | <input checked="" type="checkbox"/> Voice audio recording |
| <input type="checkbox"/> Other:  |  |   |

### Identifying numbers for sole proprietors (including business information).

- |  |  |   |
|--|--|---|
| <input checked="" type="checkbox"/> Sole proprietor business credit card number          | <input checked="" type="checkbox"/> Business Phone or Fax Number                           | <input checked="" type="checkbox"/> Business Physical/Postal Mailing Address                |
| <input checked="" type="checkbox"/> Sole proprietor business professional license number | <input checked="" type="checkbox"/> Sole proprietor business file case number              | <input checked="" type="checkbox"/> Sole proprietor business taxpayer identification number |
| <input checked="" type="checkbox"/> Sole proprietor business license plate number        | <input checked="" type="checkbox"/> Sole proprietor business vehicle identification number | <input checked="" type="checkbox"/> Sole proprietor business bank account number            |
| <input checked="" type="checkbox"/> Other: Business e-mail address                       | <input checked="" type="checkbox"/> Other: Business Cell Number                            | <input type="checkbox"/> Other:   |

## Section 3.3 Sources from which PII is obtained

### 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.
- Retired federal employees.
- Former Treasury employees.
- Federal contractors, grantees, interns, detailees etc. PII is received via paper formats other than a form, system inputs, email, scanned documents, extracted from a technology
- Federal job applicants.
- Other:

### **Current Federal Employees, Interns, and Detailees**

- Current Federal employees providing information in their capacity as federal employees
- Interns. PII may be collected from various formats (i.e., paper format other than a form, portable devices, email, scanned documents, extracted from technology such as PIV card readers) to respond to discovery requests.
- Detailees. PII may be collected from various formats (i.e., paper format other than a form, portable devices, email, scanned documents, extracted from technology such as PIV card readers) to respond to discovery requests.
- Other employment-related positions. Contractors working for the OCC. PII may be collected from various formats (i.e., paper format other than a form, portable devices, email, scanned documents, extracted from technology such as PIV card readers) to respond to discovery requests.

### **Treasury Bureaus (including Departmental Offices)**

- Other Treasury Bureaus: Financial Crimes Enforcement Network (FinCEN) primarily, but other bureaus as necessary. Incidental PII may be collected via various formats (i.e., paper format other than a form, portable devices, Internet, email, scanned documents, bulk transfers, notes from a phone interview or face to face contact) to be used in investigations of wrongdoing.

### **Other Federal Agencies**

- Other federal agencies: Other regulatory agencies (e.g., Federal Reserve Board (FRB), Consumer Financial Protection Bureau (CFPB), Federal Deposit Insurance Corporation (FDIC)); law enforcement agencies (e.g., DOJ, FBI); and Congress, as necessary. Incidental PII may be collected via various formats (i.e., paper format other than a form, portable devices, email, scanned documents, notes from a phone interview or face to face contact) in response to subpoenas, to respond to discovery, to conduct parallel investigations or enforcement actions or to refer violations of law, Congressional requests for information.

### **State and Local Agencies**

- State and local agencies: State Courts, Agencies, and Regulatory Bodies, as necessary. Incidental PII may be collected in response to discovery requests, subpoenas, and court

orders as part of state litigation, or other Requests for Information permitted under federal law, regulation, or written agreement.

### Private Sector

Private sector organizations: Banks, financial organizations, and their representatives. Incidental PII may be collected via various formats (i.e., paper format other than a form, portable devices, Internet, email, scanned documents, extracted from technology, notes from a phone interview or face to face contact) as part of data submitted subject to OCC's supervision of such organizations.

### Other Sources

Other sources not covered above: Administrative Courts, Other Third Parties (e.g., individuals, private organizations). Incidental PII may be collected via various formats (i.e., paper format other than a form, portable devices, email, scanned documents, extracted from technology, notes from a phone interview or face to face contact) to respond to discovery requests, subpoenas, court order as part of administrative litigation, or to obtain information from third parties that is relevant to the subject matter of claims, civil proceedings, or administrative actions involving the OCC, per 81 FR 2945, 2956 (2016).

## Section 3.4: Privacy and/or civil liberties risks related to collection

### Section 3.4(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.
2.  Some or  all of the information in this system was collected directly from an individual to whom it pertains.

### Section 3.4(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. OCC may gather incidental PII directly from a respondent to a subpoena, part of subpoena, or discovery request authorized by a federal or administrative court. The PII maintained in this system is exempt from requiring the Privacy Act Statement per 31 CFR 1.36, Litigation Information System (CC .510).

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 OCC 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 3.4(c) Use of Full Social Security Numbers**

#### ***3.4(c)i. Justification of Social Security Numbers***

1.  N/A No full SSNs are maintained in the system.
2.  Full SSNs are maintained in the system and the following approved Treasury uses of SSNs apply: The system contains social security numbers; however, it does not use the SSN as a personal identifier. SSNs are collected incidentally as part of documentation shared by the data source (individual or organization).
  - 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.

#### ***3.4(c)ii. Controls implemented to limit access to and or improper disclosure of full Social Security Numbers***

1.  Full SSNs are ***not*** maintained in the system.
2.  Full SSNs ***are*** maintained in the system 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.

- b.  do not require the SSN to perform their official duties.  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: Full or truncated SSNs are downloaded in documents provided and reviewed for investigatory or litigation purposes. The SSNs are incidental and not used as part of the investigation or litigation.

**3.4(c)iii Denial of rights, benefits, or privileges for refusing to disclose Social Security Number**

- 1.  N/A No SSNs are maintained in the system.
- 2.  Full SSNs are collected, but no individual will be denied any right, benefit, or privilege provided by law if the individual refuses to disclose their SSN for use in the system. The agency is not responsible for providing or denying any right, benefit, or privilege provided by law.
- 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:
  - 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 3.4(d) Records describing how individuals exercise First Amendment rights**

- 1.  N/A. The system does ***not*** maintain information describing how an individual exercises their rights guaranteed by the First Amendment.

2.  The system ***does*** maintain information describing how an individual exercises their rights guaranteed by the First Amendment.
  - a.  The individual about whom the information was collected or maintained expressly authorizes its collection/maintenance;
  - b.  The information maintained is pertinent to and within the scope of an authorized law enforcement activity because;
  - c.  The following statute expressly authorizes its 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**

#### **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 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.  All  Some of the PII maintained in the system is part of a system of records and ***is*** exempt. The exemption claimed for these records is appropriate because it is used for investigation and litigation purposes. See 66 FR 54175-01, 2001 (NPRM) and 31 C.F.R. 1.36. As noted in the NPRM, application of the requirements of (e)(5) to this system of records would hinder the initial collection of any information that could not, at the moment of collection, be determined to be accurate, relevant, timely, and complete. Similarly, application of this provision would seriously restrict the OCC's ability to disseminate information pertaining to a possible violation of law to law enforcement and other regulatory agencies. It is often impossible or unfeasible to determine accuracy, relevance, timeliness, or completeness prior to the collection of the information or prior to the dissemination. In addition, information that may initially appear inaccurate, irrelevant, untimely, or incomplete may, when collated and analyzed with other available information, become more pertinent as an investigation progresses.
3.  The PII maintained in the system 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*].  ***None*** of the information maintained in the system is part of a system of records. 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 that is part of a [system of records](#) is exempt.

2.  For all information maintained in the system that is part of a system of records that is exempt, 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: investigation and litigation purposes.
  - 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 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 are given an opportunity to explain or modify their information (*check one*)  before  after the adverse determination is made.
  - e.  Other:
  
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.**

1.  The records maintained by this system are ***not*** used to make any adverse determinations about individuals
2.  The records maintained by this system ***are*** used to make adverse determinations about individuals ***and***:
  - a.  These records ***were*** exempted from the Privacy Act provision that requires collection directly from the subject individual to the greatest extent practicable.
  - b.  These records were ***not*** exempted from the requirement to collect information directly from the individual to the greatest extent practicable ***and***
    - i.  ***All*** records used to make an adverse determination are collected directly from the individual about whom the decision is made.  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.
    - 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 :
      - 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:.

**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:  The PII collected for use in the system is NOT used to make adverse determinations about an individual's rights, benefits, and privileges under federal programs.

- b.  The records maintained in the system 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.  OCC has published regulations in place describing how individuals may seek access to and amendment of their records under the [Privacy Act](#).
- d.  Individuals who provide their information directly to OCC for use in the system are provided notice of the adverse determination and an opportunity to amend/correct/ update their information  before  after it is used to make a final, adverse determination about them.
- e.  Individuals who provide their information directly to OCC for use in the system 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.
- 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.
- g.  Other:

***Technical controls***

- 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).
- c.  Technical and/or administrative controls put are 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.
- d.  Address verification and correction software.
- e.  Other: Appropriate security and chain of custody controls protect information from loss and ensure content remains unchanged from the time it was obtained. Banks use BankNet, a secure file transfer protocol, to submit data that includes PII to

the agency. The agency uses encrypted hard drives and secure file transfer protocol to upload data to the vendor supported (FedRAMP authorized) cloud applications

## Section 4.2 Data-Mining

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

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

1.  The PII maintained in the system ***is not*** part of a Privacy Act system of records.
2.  The information maintained in the system ***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 ***is*** part of a Privacy Act system of records and ***is*** used as part of a matching program.

**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](#).

**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 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.

- 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 OCC) organizations and individuals**

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

- 1.  PII maintained in the system is **not** shared with agencies, organizations, or individuals external to Treasury.
- 2.  PII maintained in the system **is** shared with the following agencies, organizations, or individuals external to the OCC: PII is shared with Federal agencies (e.g., Treasury bureaus, FinCEN, CFPB, DOJ), regulatory bodies, and Congress; federal, state, and administrative courts; and other Third Parties (e.g., individuals, private organizations)
- 3.  All external disclosures **are** authorized by the Privacy Act (including routine uses in the applicable SORN).

##### **Section 4.4(b) Accounting of Disclosures**

###### ***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 **is** exempt from the requirement to make the accounting available to the individual named in the record. Exemption from this requirement was claimed because: 31 CFR 1.36 maintained in the system in response to subpoenas, discovery, Congressional requests for information, or with other federal agencies for the purpose of parallel investigations or enforcement actions or to refer violations of law.
- 4.  The Privacy Act system of records maintained in the system 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 OCC) and the name and address of the person or agency to whom the disclosure is made.
- 5.  The Privacy Act system of records maintained in the system 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(c) Obtaining Consent Prior to New Disclosures Not Authorized by the Privacy Act**

##### ***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 the OCC 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.

#### **Section 5: Compliance with federal information management requirements**

##### **Section 5.1: The Paperwork Reduction Act**

1.  The system 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)  The system involves a new collection of [information in identifiable form](#) for 10 or more persons from outside the federal government.
3.  The system completed an Information Collection Request ("ICR") and received OMB approval.
4.  The system did not complete an Information Collection Request ("ICR") and receive OMB approval because LSS does not collect information from individuals using an identifiable form. The system stores information collected from institutions or collected from individuals by subpoena or other individualized information requests, so an ICR is not applicable.

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

1.  The records used in the system are covered by a NARA's General Records Schedule (GRS).
2.  The records used in the system are covered by a NARA approved Treasury bureau Specific Records Schedule (SRS). The SRS is the OCC Comprehensive Records Retention Schedule, August 1, 2008.
3.  The system owner sought approval from NARA for an SRS and is awaiting a response from 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**



1.  The system is a federal [information system](#) subject to FISMA requirements.
2.  The system last completed an SA&A and received an ATO on: 8/31/2021.
3.  This is a new system has not yet been authorized to operate.
4.  The system 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 OCC duties. Users are granted access that is requested by case leads and approved by management. Case leads also review access control lists semiannually to ensure unauthorized users have not been granted access to information.
5.  All OCC security requirements are met when disclosing and transferring information (e.g., bulk transfer, direct access by recipient, portable disk, paper) from the Treasury system to internal or external parties.
6.  This system maintains an audit log of system users to ensure they do not violate the system and/or OCC Rules of Behavior. Case leads review audit logs monthly to ensure unauthorized users do not access information. Audit logs are used to ensure only authorized users have accessed documents stored within the LSS.
7.  This system 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.

#### Section 5.4: Section 508 of the Rehabilitation Act of 1973

1.  The 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 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 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 is not in compliance with all [Section 508](#) requirements. The following actions are in progress to ensure compliance: where product features or components are not fully accessible, the agency is required to make available, upon request, an alternative means of accessing the information or functions supported.

**Responsible Officials  
Approval Signature**

*Signed Copy On File*

---

**FOR PUBLIC COPY**

Privacy Program Manager

Date signed: 3/21/2022