

CIRCULAR

DATE June 17, 2020

RECORDS SYSTEMS SUBJECT TO THE PRIVACY ACT

REVIEW DATE: June 17, 2025

1.0 PURPOSE AND SCOPE

This circular provides guidance on the maintenance of records subject to the Privacy Act of 1974 (Privacy Act). The circular providing guidance pertaining to the rights to notification, access, accounting for disclosures, and requests for amendment of Privacy Act records is Circular No. 50-00.8, "Processing Requests under the Freedom of Information and Privacy Acts," dated December 16, 2015.

This circular applies to all records contained in a Privacy Act system of records, and maintained by the employees and contractors of the Bureau of Engraving and Printing (Bureau/BEP) in the Washington, DC Facility (DCF) and Western Currency Facility (WCF).

2.0 POLICY

- 2.1 The purpose of the Privacy Act is to provide certain safeguards for an individual against an invasion of personal privacy by any executive department, military department, government corporation, government controlled corporation, or other establishment in the executive branch of the United States Government (including the Executive Office of the President), or any independent regulatory agency.
- 2.2 The Privacy Act focuses on four policy objectives:
 - 2.2.1 To establish a code of fair information practices that requires agencies to comply with statutory norms for collection, maintenance, and dissemination of records.
 - 2.2.2 To restrict disclosure of any item, collection, or grouping of information about an individual maintained by agencies.
 - 2.2.3 To grant individuals increased rights of access to records maintained about them.
 - 2.2.4 To grant individuals the right to seek amendment of records maintained about them upon a showing that the records are not accurate, relevant, timely or complete.
- 2.3 It is the policy of the BEP to:
 - 2.3.1 Maintain Privacy Act records in accordance with the Privacy Act, applicable federal agency-wide regulations (e.g., Department of Justice, Office of Management and Budget), and the Department of the Treasury's Privacy Act regulation and policies.

CIRCULAR

DATE June 17, 2020

-
- 2.3.2 Make all BEP employees and contractors involved in the design, development, operation, or maintenance of a Privacy Act system of records aware of and comply with the Privacy Act, applicable federal agency-wide regulations (e.g., Department of Justice, Office of Management and Budget), and the Department of the Treasury's Privacy Act regulation and policies. Any BEP employee or contractor who willfully maintains a Privacy Act system of records without meeting the proper notice requirements, or willfully discloses information subject to the Privacy Act to an unauthorized recipient shall be guilty of a misdemeanor and subject to a fine up to \$5,000.
- 2.3.3 Disclose any record contained in a Privacy Act system of records to a recipient agency or non-federal agency for use in a computer matching program pursuant to an approved computer matching agreement.
- 2.3.4 Not to collect, maintain, use, or disseminate information describing how an individual exercise rights guaranteed by the first amendment, the individual's religious or political beliefs or activities, or membership in association or organization unless the maintenance of such record is: (1) expressly authorized by statute; (2) expressly authorized by the individual about whom the records is maintained; or (3) pertinent to and within the scope of an authorized law enforcement activity per 5 USC 552a (e)(7).
- 2.3.5 To collect information about an individual primarily from that individual.
- 2.3.6 Not to collect information of personal nature from individuals unless authorized to collect it to achieve or carry out BEP's mission, functions or responsibilities.
- 2.3.7 To collect from individuals, information that is only necessary to carry out BEP's mission, function or responsibilities.
- 2.3.8 Provide the required Privacy Act statement whenever an individual is asked to supply information about themselves or a family member. This requirement not only applies to pre-printed forms such as an application for a position or a benefit, but sign-in logs and all other documents that require an individual to disclose an identification number or some identifying symbol. The Privacy Act statement should also be provided verbally when information is being collected by an interview, subject to any exemption from the provisions of the Privacy Act.
- 2.3.9 Not to deny any right, benefit, or privilege provided by law to any individual because of that individual's refusal to disclose their social security number. However, this does not apply if the disclosure is required by statute; or the disclosure of a social security number 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 before that date for the purpose of verifying identify. In case BEP asks an

CIRCULAR

DATE June 17, 2020

individual to disclose their social security number, BEP will inform the individual whether disclosure is mandatory or voluntary; and what uses will be made of it.

- 2.3.10 Not to sell or rent an individual's name and address unless such action is specifically authorized by law. This is not to be construed to require the withholding of names and addresses otherwise permitted to be made public.

3.0 SUPERSESSION

This circular supersedes Circular No. 50-00.7, dated January 21, 2011, entitled "Record Systems Subject to the Privacy Act."

4.0 DEFINITIONS

- 4.1 Individual – A citizen of the United States of America or an alien lawfully admitted for permanent residence.
- 4.2 Maintain – Includes maintain, collect, use, or disseminate.
- 4.3 Record – Any item, collection, or grouping of information about an individual that is maintained by BEP including, but not limited to the individual's education, financial transactions, medical history, and criminal or employment history and that contains their name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.
- 4.4 System of Records – A group of any records under the control of the BEP from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual.
- 4.5 Routine Use – With respect to the disclosure of a record, the use of such record for a purpose, which is compatible with the purpose for which it was collected.
- 4.6 Privacy and Civil Liberties Impact Assessment (PCLIA) – An analysis of how information is handled to (1) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (2) determine the risks and effects of creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, and disposing of information in identifiable form in an electronic information system, and (3) examine and evaluate protections and alternate processes for handling information to mitigate potential privacy concerns. A PCLIA is both an analysis and a formal document detailing the process and the outcome of the analysis.

5.0 AUTHORITIES AND REFERENCES

- 5.1 The Privacy Act of 1974, [5 United States Code \(USC\) § 552a](#).

CIRCULAR

DATE June 17, 2020

-
- 5.2 [The Computer Matching and Privacy Protection Act of 1988](#), 5 USC § 552a(o).
 - 5.3 E-Government Act of 2002, 44 USC § 101.
 - 5.4 [Office of Management and Budget \(OMB\), Privacy Act Implementation, Guidelines and Responsibilities](#), 40 Fed. Reg. 28948 (July 9, 1975).
 - 5.5 [OMB Circular No. A-108](#), Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act.
 - 5.6 [OMB Circular No. A-130](#), “Management of Federal Information Resources,” (November 30, 2000).
 - 5.7 OMB Bulletin 89-22, “Instructions on Reporting Computer Matching Programs to the Office of Management and Budget (OMB), Congress and the Public.”
 - 5.8 OMB Final Guidance Interpreting the Provisions of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1988, 54 Fed. Reg. 25818 (June 19, 1989).
 - 5.9 The Computer Matching and Privacy Protection Amendments of 1990 and the Privacy Act of 1974, 56 Fed. Reg. 18599 (April 23, 1991).
 - 5.10 OMB M-13-20, “Protecting Privacy while Reducing Improper Payments with the Do Not Pay Initiative.”
 - 5.11 [Department of the Treasury Privacy Act Regulation, 31 Code of Federal Regulations \(CFR\), Part 1, Subpart C, “Privacy Act.”](#)
 - 5.12 [Department of the Treasury Employee Rules of Conduct, 31 CFR Part 0.](#)
 - 5.13 [Treasury Directive TD 25-04](#), “The Privacy Act of 1974, as amended”, dated August 26, 2010 (Administrative Edit: January 27, 2014).
 - 5.14 [Treasury Directive Publication TDP 25-04](#), “The Privacy Act Handbook.”
 - 5.15 [Department of the Treasury Directive TD 25-06](#), “The Treasury Data Integrity Board,” dated January 26, 2015.
 - 5.16 Department of the Treasury Publication TDP 25-06, “Computer Matching Handbook.”
 - 5.17 Department of the Treasury, “Removal of Information,” TDF 80-05.5 (Rev. 8/2016).
 - 5.18 [Government-wide System of Records Notice.](#)
 - 5.19 [Treasury-wide System of Records Notice.](#)
 - 5.20 [BEP System of Records Notice.](#)
 - 5.21 [Notices for Approved Computer Matching Programs Agreements.](#)
 - 5.22 [National Archives and Records Administration \(NARA\) General Records Schedule.](#)
 - 5.23 [BEP Records Schedule.](#)

CIRCULAR

DATE June 17, 2020

5.24 Department of Justice, Overview of the Privacy Act of 1974.**6.0 RESPONSIBILITIES**

- 6.1 The Department of the Treasury (Department/Treasury), Assistant Secretary for Management (ASM) is BEP's Chief Privacy and Civil Liberties Officer, as well as the Senior Agency Official for Privacy (SAOP).
- 6.2 The Deputy Assistant Secretary for Privacy, Transparency and Records (DASPTR) at Treasury is the principal advisor to the ASM in their role as the Chief Privacy and Civil Liberties Officer for all Treasury bureaus. The DASPTR approves and submits reports on new or altered Privacy Act system of records notices of BEP to the Office of Management and Budget and Congress. The DASPTR authority may not be delegated.
- 6.3 The Director of the Office of Privacy and Civil Liberties at Treasury represents and reports to the DASPTR on all matters relating to the Privacy Act, as well as to:
- 6.3.1 Manage the implementation of the Privacy Act within Treasury;
 - 6.3.2 Issue and revise, as needed Treasury's Privacy Act regulation applicable to all bureaus;
 - 6.3.3 Provide appropriate Treasury-wide Privacy Act training to employees and contractors, and training to the employees on the procedures and standards of conduct. The training shall provide suitable emphasis on the civil and criminal penalties imposed on the Department and individual employees and contractors for non-compliance with specified requirements of the Privacy Act.
 - 6.3.4 Ensure that BEP:
 - 6.3.4.1 Carries out the provisions of the Privacy Act, Treasury's Privacy Act regulation, [Treasury Directive TD 25-04](#), and OMB Circular A-130, Appendix I.
 - 6.3.4.2 In partnership with the Office of the Deputy Assistant Secretary for Information Systems and Chief Information Officer, participate on government-wide task forces on computer technology concerned with establishing or affecting policies for collecting, compiling, using, maintaining and safeguarding Federal Privacy Act system of records.
- 6.4 The Director of BEP is responsible for:
- 6.4.1 Establishing internal procedures to ensure the effectiveness of BEP's Privacy Act program and to safeguard individual privacy in the collection, compilation, maintenance, use, and dissemination of Federal records;

CIRCULAR

DATE June 17, 2020

-
- 6.4.2 Submitting the following to the Department of the Treasury, Office of Privacy, Transparency and Records for the review and approval of the DASPTR:
- 6.4.2.1 A notice and report for each new or altered system of records;
 - 6.4.2.2 A proposed and final rule for any determination to exempt a system of records from provisions of the Privacy Act;
 - 6.4.2.3 A notice and report of the establishment or alteration of a matching program; and
 - 6.4.2.4 Any proposed or final rules to existing Privacy Act regulations for review and concurrence prior to the review and concurrence procedures under TD 28-01;
- 6.4.3 Establishing procedures allowing an individual to appeal an initial adverse agency determination regarding a request for amendment of records;
- 6.4.4 Submitting to the DASPTR a copy of the Bureau's initial determination and response to an appeal regarding a request to amend records; and
- 6.4.5 Assuring BEP employees and contractors are advised of the provisions of the Privacy Act and Treasury's Privacy Act regulation, including the criminal penalties and civil liabilities provided therein, and their collective responsibilities to protect the security of personal information, to assure its accuracy, relevance, timeliness, and completeness, to avoid unauthorized disclosure either orally or in writing, and to insure that no information system concerning individuals, no matter how small or specialized is maintained without the required Federal Register public notice.
- 6.5 The Office of the Chief Counsel is responsible for:
- 6.5.1 Acting as BEP's Privacy Act Officer and administering the Privacy Act program on behalf of the Director of BEP;
 - 6.5.2 Responding to all data calls/requests from the ASM, DASPTR, Director of Privacy and Civil Liberties, OMB, NARA's Federal Register and/or Congress relating to the Privacy Act;
 - 6.5.3 Reviewing, and updating, if needed, the Federal Register notices containing the Bureau's Privacy Act system of records annually. A listing of the Government-wide, Treasury-wide, and BEP's system of records notices (SORNs) can be found in [BEP's Freedom of Information Act \(FOIA\) and Privacy Act \(PA\) programs electronic reading room and the Department of the Treasury Privacy Act home page](#);
 - 6.5.4 Preparing and submitting the following to the Director of the Department of the Treasury, Office of Privacy, Transparency and Records for the review

CIRCULAR

DATE June 17, 2020

-
- and approval of the DASPTR, OMB and Congress, and for publication in the Federal Register;
- 6.5.4.1 The Privacy Act compilation of notices of BEP's system of records. The existing notices of system of records will be published in their entirety by Treasury every three years in the Federal Register;
 - 6.5.4.2 Notices and reports on new or altered BEP system of records;
 - 6.5.4.3 Proposed and final rules for exempt BEP system of records; and
 - 6.5.4.4 Notices for computer matches agreements covered under the provisions of the Computer Matching and Privacy Protection Act of 1988.
- 6.5.5 Ensuring that the Office of Privacy and Civil Liberties at Treasury provides the annual Treasury-wide Privacy Act training to BEP employees and contractors, and training on the procedures and standards of conduct to BEP employees. The training shall provide suitable emphasis on the civil and criminal penalties imposed on the Department and individual employees and contractors for non-compliance with specified requirements of the Privacy Act;
 - 6.5.6 Providing additional role-based Privacy Act training, when appropriate and/or requested;
 - 6.5.7 Informing all BEP employees and contractors of their responsibilities under the Privacy Act, Federal agency-wide regulations (e.g., Department of Justice, Office of Management and Budget), and the Department of the Treasury's Privacy Act regulation and policies. Copies of the Privacy Act, regulations, and policies may be obtained from the [BEP FOIA/PA Electronic Reading Room](#);
 - 6.5.8 Approving and ensuring that any form, method, or format developed or used to collect information about individuals or a family member contains the required Privacy Act statement either in the form or on a separate form that can be retained by the individual. The Privacy Act statement shall inform the individual (1) the authority that authorizes the solicitation of the information, and whether disclosure of such information is mandatory or voluntary; (2) the principal purpose(s) for which the information is intended to be used; (3) the routine uses, which may be made of the information as published in the notices of system of records in the Federal Register; and (4) the effects on the individual, if any, of not providing all or any part of the requested information.
 - 6.5.9 Reviewing Privacy Threshold Analysis (PTA) when warranted and/or approving Privacy and Civil Liberties Impact Assessments (PCLIA) performed by the Government Information Specialist for Privacy to

CIRCULAR

DATE June 17, 2020

determine that privacy risks and routine uses are analyzed and evaluated, and whether additional privacy compliance documentation (e.g., SORN) are needed for new or altered existing BEP system of records. The PTA and PCLIA are required prior to commencing the SORN review/approval process for any new or altered BEP system of records. Please refer to Circular No. 25-01.1, Privacy and Civil Liberties Policies, Compliance and Responsibilities, and Safeguarding of Personally Identifiable Information (PII) for more information about the PTA and PCLIA process; and

- 6.5.10 Reviewing and approving written Computer Matching Agreements (CMA) between the source agency and the recipient agency (or non-federal agency) specifying the terms of the matching program. Any record contained in a system of records may only be disclosed to a recipient agency or non-federal agency for use in a computer matching program pursuant to a CMA between the source agency and the recipient agency (or non-federal agency). BEP's CMAs must be approved by Treasury's Data Integrity Board. In addition, notices for approved CMAs must be published in the Federal Register.
- 6.6 The BEP Government Information Specialist for Privacy within BEP's Office of Critical Infrastructure and IT Security is responsible for:
- 6.6.1 Ensuring that new or proposed changes to BEP's programs, initiatives, activities, social media, information systems, IT systems (including but not limited to the cloud environment), forms (regardless of format), methods, which result in the collection of information subject to the Privacy Act is coordinated with the Office of the Chief Counsel;
- 6.6.2 In collaboration with the Program Office and appropriate BEP stakeholders at the System Development Life Cycle (SDLC) stage, conduct and complete privacy compliance documentation (e.g., SORNs, PLCIAs, PTAs) for new or updated BEP programs, activities, social media, information systems, information technologies, or operations in accordance with federal law and regulation. The PTA and PCLIA are required prior to commencing the SORN review/approval process for any new or altered BEP system of records. Please refer to Circular No. 25-01.1, Privacy and Civil Liberties Policies, Compliance and Responsibilities, and Safeguarding of Personally Identifiable Information (PII) for more information about the PTA and PCLIA process;
- 6.6.3 Approving any form, method or format used to collect information about individuals;
- 6.6.4 Providing guidance and ensuring that the physical environment in which information is collected, stored, processed, or transmitted is sufficiently secure to protect the confidentiality of the records, and that there are sufficient system controls over access and authorization to protect

CIRCULAR

DATE June 17, 2020

-
- information and record confidentiality, as well as protect the overall integrity of the IT system;
- 6.6.5 Ensuring that when a Certification and Accreditation review is performed for an IT system or major application, Privacy Act information is identified and appropriate safeguards are in place; and
- 6.6.6 Ensuring that all automated systems containing Privacy Act information are evaluated to determine whether they have connectivity with other systems, either within or outside the Bureau and, if they do, an Interconnection Security Agreement is executed for those other systems.
- 6.7 BEP's Forms Officer in the Office of Critical Infrastructure and IT Security is responsible for:
- 6.7.1 Seeking the review and approval of the Office of the Chief Counsel and the Government Information Specialist for Privacy on all new and modified forms (regardless format used), collecting privacy information to assess whether the completion of any required documentation, such as privacy assessments, Privacy Act notices, Privacy Act statement, Paperwork Reduction Act clearance, and Federal Register notices (e.g., SORNs, PRA/OMB control numbers) are needed. See Circular No. 80-04, Forms Management Circular, dated November 23, 2018.
- 6.8 System Owners, System Managers, and/or Office Chiefs are responsible for:
- 6.8.1 Storing, using, maintaining, and destroying Privacy Act records in accordance with the provisions of the Act, Treasury's Privacy Act regulation and policies, and the Government-wide or BEP Records Schedule. The development of any plans by the system owner, system manager, and/or Office Chiefs in conjunction with BEP's Records Officer should be consistent with the intent of the Privacy Act and good record management policies and procedures and cover such areas as:
- 6.8.1.1 Administrative, technical, and physical controls for storing and safeguarding records to ensure the protection of the records system from unauthorized access or disclosure (e.g., physical security, personnel screening, etc.), and from physical damage, destruction, hazards to their security, confidentiality, or integrity, which could result in substantial harm, embarrassment,

CIRCULAR

DATE June 17, 2020

-
- inconvenience, or unfairness to any individual on whom information is maintained;
- 6.8.1.2 Categories or level of employees within the agency who have a need to have access to the records for the performance of their duties;
 - 6.8.1.3 Format or media in which the records are maintained (paper, electronic), how long the records will be maintained in their immediate office, and when they are moved to BEP's records storage room or NARA;
 - 6.8.1.4 Criteria for determining at what point the records will have satisfied the purpose for which they were collected and when and how the records will be destroyed; and
 - 6.8.1.5 Automated systems shall comply with security standards promulgated by the National Institute of Standards and Technology.
- 6.8.2 Ensuring that Privacy Act records are accurate, relevant, current, and complete.
 - 6.8.3 Reviewing their Privacy Act system of records and reporting to the Office of the Chief Counsel on the status of the Privacy Act system(s) of records annually. This report shall indicate what systems are in use, whether changes have been made to existing systems during the reporting period, or whether new systems will be developed since the last annual update.
 - 6.8.4 Informing the Office of the Chief Counsel of any new or proposed changes to existing Privacy Act system(s) of records to determine whether a the publication of a Federal Register notice (e.g. SORN) or other privacy compliance documentation is required. Implementation of new or changes to an existing Privacy Act system of records must await the publication of the Federal Register notice before BEP collects the information about individuals. Therefore, no creation, development, changes, or additions shall be made to a Privacy Act system(s) of records without first seeking approval of the Office of the Chief Counsel. Any BEP employee or contractor who willfully maintains a Privacy Act system of records without meeting the proper Federal Register notice requirements shall be guilty of a misdemeanor and subject to a fine up to \$5,000.
 - 6.8.5 Obtaining the Bureau's Forms Officer, the Government Information Specialist for Privacy, and the Office of the Chief Counsel approval prior to developing, modifying, or using any forms, methods, or format used to collect information from individuals about themselves. The program office issuing the form is responsible for the preparation of the Privacy Act statement for the review and approval of the Office of the Chief Counsel.

CIRCULAR

DATE June 17, 2020

-
- 6.8.6 Providing accurate information needed to perform a PTA and PCLIA prior to commencing the SORN review/approval process with the Office of the Chief Counsel when planning, developing, implementing, updating, and/or operating BEP's programs, forms, activities, social media, information systems, information technologies, social media or operations etc. System owners and managers shall perform and cooperate with the Government Information Specialist for Privacy to complete the required PTA and PCLIA.
- 6.8.7 Ensuring that their employees and contractors, who are involved in the design, development, operation, or maintenance of a Privacy Act system of records, obtain training and are aware of the requirements of the Privacy Act, Federal agency-wide regulations (e.g., Department of Justice, Office of Management and Budget), and Treasury's Privacy Act regulation and policies.
- 6.8.8 Ensuring that BEP contractors comply with the contract requirements relating to privacy. Contracts should contain the standard contract requirements found at 48 CFR Ch.1, Part 24.1, to ensure compliance with the Privacy Act. Training and necessary clearances will precede the engagement of government contractors to the individuals accessing Privacy Act records. Strict care must be used to ensure that BEP contractors are given only the minimum access to data that is necessary, and that they have no opportunity to access data beyond that which is intended that they access.
- 6.8.9 Initially determining when information about individuals needs to be collected, what the policy objectives to be served by the collection are, and whether the collection is authorized by a statute, Executive Order, and/or regulation. In assessing the need for the information the system manager, system owner, and/or Office Chiefs should consider whether the agency really needs to use information that is individually identifiable or would a sampling procedure or other non-specific process suffice. The assessment should also consider what the financial cost associated with maintaining the information is, and what the risks or adverse consequences are to the Bureau of not collecting the information.
- 6.9 BEP employees and contractors who are involved in the design, development, operation or maintenance of any Privacy Act system of records are responsible for:
- 6.9.1 Completing the annual Treasury-wide privacy awareness training when assigned via the Treasury Integrated Talent Management learning tool. This training provides suitable emphasis on the civil and criminal penalties imposed on the Department and individual employees for non-compliance with specified requirements of the Privacy Act.
- 6.9.2 Complying with federal laws and regulations and agency and Treasury-wide policies concerning Privacy Act and Treasury's rules of conduct.

BUREAU OF ENGRAVING AND PRINTING

CIRCULAR

DATE June 17, 2020

- 6.9.3 Following Treasury's rules of conduct and best practices and procedures concerning record keeping to safeguard Privacy Act records entrusted to them in the performance of their official duties.
- 6.9.4 Advising their supervisors of the existence or contemplated development of any Privacy Act system of records, which is capable of retrieving information about individuals by individual identifiers.

7.0 OFFICE OF PRIMARY RESPONSIBILITY

Office of the Chief Counsel

<electronically approved>

Leonard R. Olijar

Director