



Privacy and Civil Liberties Impact Assessment
for the
Manufacturing Support Suite (MSS)

July 26, 2019

Bureau Reviewing Official

Michael Pease

Chief, Office of Critical Infrastructure and IT Security
Office of the Chief Information Officer
Bureau of Engraving and Printing
Department of the Treasury

Bureau Privacy Official

Anthony Johnson

Government Information Specialist (Privacy)
Office of Critical Infrastructure and IT Security
Cyber Security Policy and Compliance Division
Bureau of Engraving and Printing
Department of the Treasury

Section 1: Introduction

The Bureau of Engraving and Printing (BEP's) is preparing this PCLIA following a reassessment of the information maintained in the Manufacturing Support Suite (MSS) System.

BEP uses MSS to manage: (1) acquisitions/procurement processes; (2) numismatic products public sales; (3) currency notes and security documents manufacturing activities, and (4) accounting, budgeting, audits, financial payment processing (e.g. travel reimbursement claims), and financial reporting functions. MSS maintains Personally Identifiable Information (PII) of BEP employees/contractors and members of the public that is relevant and necessary to fulfill BEP's mission of developing and producing U.S. currency notes and security documents.

Section 2: Definitions

Agency – means any entity that falls within the definition of the term “executive agency” as defined in 31 U.S.C. § 102.

Certifying Official – The Bureau Privacy and Civil Liberties Officer(s) who certify that all requirements in TD and TD P 25-07 have been completed so a PCLIA can be reviewed and approved by the Treasury Deputy Assistant Secretary for Privacy, Transparency, and Records.

Collect (including “collection”) – means the retrieval, receipt, gathering, or acquisition of any PII and its storage or presence in a Treasury system. This term should be given its broadest possible meaning.

Contractors and service providers – are private companies that provide goods or services under a contract with the Department of the Treasury or one of its bureaus. This includes, but is not limited to, information providers, information processors, and other organizations providing information system development, information technology services, and other outsourced applications.

Data mining – means a program involving pattern-based queries, searches, or other analyses of 1 or more electronic databases, where – (a) a department or agency of the federal government, or a non-federal entity acting on behalf of the federal government, is conducting the queries, searches, or other analyses to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals; (b) the queries, searches, or other analyses are not subject-based and do not use personal identifiers of a specific individual, or inputs associated with a specific individual or group of individuals, to retrieve information from the database or databases; and (c) the purpose of the queries, searches, or other analyses is not solely – (i) the detection of fraud, waste, or abuse in a government agency or program; or (ii) the security of a government computer system.

Disclosure – When it is clear from its usage that the term “disclosure” refers to records provided to the public in response to a request under the Freedom of Information Act (5 U.S.C. § 552, “FOIA”) or the Privacy Act (5 U.S.C. § 552a), its application should be limited in that manner. Otherwise, the term should be interpreted as synonymous with the terms “sharing” and “dissemination” as defined in this manual.

Dissemination – as used in this manual, is synonymous with the terms “sharing” and “disclosure” (unless it is clear from the context that the use of the term “disclosure” refers to a FOIA/Privacy Act disclosure).

E-Government – means the use of digital technologies to transform government operations to improve effectiveness, efficiency, and service delivery.

Federal information system – means a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information owned or under the control of a federal agency, whether automated or manual.

Final Rule – After the NPRM comment period closes, the agency reviews and analyzes the comments received (if any). The agency has the option to proceed with the rulemaking as proposed, issue a new or modified proposal, or withdraw the proposal before reaching its final decision. The agency can also revise the supporting analyses contained in the NPRM (e.g., to address a concern raised by a member of the public in response to the NPRM).

Government information – means information created, collected, used, maintained, processed, disseminated, or disposed of by or for the federal government.

Individual – means a citizen of the United States or an alien lawfully admitted for permanent residence. If a question does not specifically inquire about or an issue does not clearly involve a Privacy Act system of records, the term should be given its common, everyday meaning. In certain contexts, the term individual may also include citizens of other countries who are covered by the terms of an international or other agreement that involves information stored in the system or used by the project.

Information – means any representation of knowledge such as facts, data, or opinions in any medium or form, regardless of its physical form or characteristics. This term should be given the broadest possible meaning. This term includes, but is not limit to, information contained in a Privacy Act system of records.

Information technology (IT) – means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use: (i) of that equipment; or (ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product. It includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but does not include any equipment acquired by a federal contractor incidental to a federal contract. Clinger-Cohen Act of 1996, 40 U.S.C. § 11101(6).

Major Information system – embraces “large” and “sensitive” information systems and means “a system or project that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in

the administration of agency programs, finances, property, or other resources.” OMB Circular A-130, § 6.u. This definition includes all systems that contain PII and are rated as “MODERATE or HIGH impact” under Federal Information Processing Standard 199.

National Security systems – a telecommunications or information system operated by the federal government, the function, operation or use of which involves: (1) intelligence activities, (2) cryptologic activities related to national security, (3) command and control of military forces, (4) equipment that is an integral part of a weapon or weapons systems, or (5) systems critical to the direct fulfillment of military or intelligence missions, but does not include systems used for routine administrative and business applications, such as payroll, finance, logistics, and personnel management. Clinger-Cohen Act of 1996, 40 U.S.C. § 11103.

Notice of Proposed Rule Making (NPRM) – the Privacy Act (Section (J) and (k)) allow agencies to use the rulemaking process to exempt particular systems of records from some of the requirements in the Act. This process is often referred to as “notice-and-comment rulemaking.” The agency publishes an NPRM to notify the public that the agency is proposing a rule and provides an opportunity for the public to comment on the proposal before the agency can issue a final rule.

Personally Identifiable Information (PII) –any information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

Privacy and Civil Liberties Impact Assessment (PCLIA) – a PCLIA is:

- (1) a *process* conducted to: (a) identify privacy and civil liberties risks in systems, programs, and other activities that maintain PII; (b) ensure that information systems, programs, and other activities comply with legal, regulatory, and policy requirements; (c) analyze the privacy and civil liberties risks identified; (d) identify remedies, protections, and alternative or additional privacy controls necessary to mitigate those risks; and (e) provide notice to the public of privacy and civil liberties protection practices.
- (2) a *document* that catalogues the outcome of that privacy and civil liberties risk assessment process.

Protected Information – as the term is used in this PCLIA, has the same definition given to that term in TD 25-10, Section 4.

Privacy Act Record – any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, the individual’s education, financial transactions, medical history, and criminal or employment history and that contains the individual’s name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph. 5 U.S.C. § 552a (a)(4).

Reviewing Official – The Deputy Assistant Secretary for Privacy, Transparency, and Records who reviews and approves all PCLIA’s as part of her/his duties as a direct report to the Treasury Senior Agency Official for Privacy.

Routine Use – with respect to the disclosure of a record outside of Treasury (i.e., external sharing), the sharing of such record for a purpose which is compatible with the purpose for which it was collected 5 U.S.C. § 552a(a)(7).

Sharing – any Treasury initiated distribution of information to government employees or agency contractors or grantees, including intra- or inter-agency transfers or exchanges of Treasury information, regardless of whether it is covered by the Privacy Act. It does not include responses to requests for agency records under FOIA or the Privacy Act. It is synonymous with the term “dissemination” as used in this assessment. It is also synonymous with the term “disclosure” as used in this assessment unless it is clear from the context in which the term is used that it refers to disclosure to the public in response to a request for agency records under FOIA or the Privacy Act.

System – as the term used in this manual, includes both federal information systems and information technology.

System of Records – a group of any records under the control of Treasury from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. 5 U.S.C. § 552a (a)(5).

System of Records Notice – Each agency that maintains a system of records shall publish in the *Federal Register* upon establishment or revision a notice of the existence and character of the system of records, which notice shall include: (A) the name and location of the system; (B) the categories of individuals on whom records are maintained in the system; (C) the categories of records maintained in the system; (D) each routine use of the records contained in the system, including the categories of users and the purpose of such use; (E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records; (F) the title and business address of the agency official who is responsible for the system of records; (G) the agency procedures whereby an individual can be notified at her/his request if the system of records contains a record pertaining to him; (H) the agency procedures whereby an individual can be notified at her/his request how she/he can gain access to any record pertaining to him contained in the system of records, and how she/he can contest its content; and (I) the categories of sources of records in the system. 5 U.S.C. § 552a (e)(4).

System Owner – Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of a system.

Section 3: System Overview

Section 3.1: System/Project Description and Purpose

The BEP Manufacturing Support Suite (MSS) is an integrated set of five Information Technology (IT) applications deployed within the BEP Enterprise Network (BEN) framework that supports multiple BEP daily business activities and streamlines operational processes.

Several BEP program offices use MSS in their functional areas to accomplish BEP’s mission and objectives associated with (1) acquisitions/procurement management processes; (2) numismatic products public sales; (3) accounting, budgeting, audits, financial payment processing, and financial reporting functions; (4) currency notes and security documents manufacturing activities,

which include work order creation and management, engraving activities, equipment maintenance, materials and inventory management and accountability, and environmental health, and safety management; (5) currency quality assurance management; and (6) manufacturing standards compliance management.

After BEP employees and contractors log into MSS, the system directs the individual automatically to the specific application pertaining to their program office responsibility and user role. Once the user populates data (including PII) into the specific application administered by each program office, the data and PII resides within a secure MSS centralized database. Users may access/retrieve data pertaining specifically to their area of responsibility and user role on subsequent entries into the application.

The five IT applications within MSS are:

1) Contract Lifecycle Management (CLM)/iProcurement Application (CLM/iProcurement)

The Office of Acquisition (OA) uses the CLM/iProcurement application to support the procurement process for production-related materials, spare parts and as an inventory management tool to meet BEP's procurement requirements. It also uses CLM/iProcurement to manage suppliers and purchasers in accordance with federal acquisition regulation. CLM/iProcurement allows OA employees and contractors to:

- Manage contracts/awards
- Create and process requisitions
- Enter purchase orders
- Manage inventory items
- Manage vendor records
- Manage deliverables
- Track and manage suppliers/purchasers (buyers)
- Create and track solicitations
- Manage workflows/approvals
- Transmit acquisition/procurement reports

Federal acquisitions regulation and procedures allow BEP to limit the amount of PII collected of members of the public during the procurement and contract award processes. The Department of the Treasury, Bureau of Fiscal Services (BFS) Collections Information Repository (CIR) System collects PII from business entities from source systems such as Pay.gov and sends the PII below to the CLM/iProcurement application in order to conduct transactions with these business entities.

BEP also submits reports that include PII and statistical data on all procurement/contract actions to the GSA Federal Procurement Data System (FPDS) to permit the federal government to measure and assess the impact of federal procurement on the nation's economy, learn how awards are made to businesses in various socioeconomic categories, understand the impact of full and open competition on the acquisition process, and address changes to procurement policy.

2) Public Sales Application

The Office of External Relations (OEX) employees and contractors use the Public Sales application to store information of numismatic and engraved products sales, fulfill and ship orders, and to track orders and inventory for replenishment purposes. OEX will also use the information to maintain a mailing list of customers and interested parties to provide continuous communication and/or promotional materials about existing and upcoming product offerings. The orders for numismatic products are received via (1) telephone, (2) postal mail, (3) email, or (4) in-person at the BEP Gift Shop. The U.S. Mint (the Mint) manages the online orders for BEP numismatic products. The information will also be used to remind customers to use the Mint online catalog.

OEX intends to collect new PII of members of the public placing orders for numismatic products via (1) telephone (2) postal mail, and (3) email only. OEX collects credit card information from members of the public making in-person purchases at the BEP Gift Shop or by phone. However, OEX does not store credit card information in the Public Sales application and rather transmit the information directly to the BFS Card Acquiring Service (CAS) System to process payments manually. Bulk sales are processed by email in order to obtain the requested products and to provide a price quote. OEX does not collect bank account information for bulk sales. OEX provides the purchaser Treasury Department financial accounting data (Account and Routing Numbers) and directs the individual or entity to the BFS CIR System for direct payment processing. As a result, BEP will update its Privacy Act System of Records Notice covering numismatic products public sales (i.e. Treasury/BEP .045) to include telephone number, email address, order information (item, price, quantity, order number, order date, and order quote), currency type, customer number, and inventory data prior to collecting the data and storing it in the Public Sales application.

In addition, OEX will store non-PII statistical and inventory data resulting from the online sales. The Mint will not transfer PII from these sales back to BEP but submit statistical and inventory data for BEP to analyze product success, manage items sold, cost, and to facilitate product replenishment.

3) Office of Financial Management (OFM) Application

The Office of Financial Management (OFM) uses the OFM application to perform accounting, budgeting, audits, financial reporting functions, accounts payable/receivable and invoice transactions, and non-payroll payments or reimbursements (e.g., travel) to BEP employees.

To conduct payments to business entities, vendors, and suppliers, OFM employees use the information obtained from BFS CIR to build a MSS Payee/Supplier Record that contains information such as Tax ID numbers, banking/financial information, contact information, and voucher information.

To conduct payments to BEP personnel, OFM employees access the U.S. Department of Agriculture National Finance Center (NFC) System through the Bureau of Fiscal Services

Financial Management Service (BEP FMS) to retrieve identifying information (including the employee's Social Security number (SSN)) and to obtain banking/electronic funds transfer information in order to manually add the data to an MSS Employee HR Record comprised of the SSN, Employee ID number, banking, and contact information. This transaction allows BEP to conduct non-payroll related payments or reimbursements to employees. Upon receiving notification that an employee requires a payment or reimbursement based on the submission of a travel or other financial claim through separate channels, an OFM employee creates a MSS Payee/Supplier Record using an interface between the two records. The Payee/Supplier Record auto-populates the Employee ID number field, which is used in lieu of the employee's SSN for payment processing and contains information needed to process the payment. The Payee/Supplier Record contains the payee's identifying information, banking information, contact information, and agency accounting information to align the payments/reimbursements to the correct BEP office/operating unit's financial account. The Payee/Supplier Record alleviates the need to use the SSN to conduct subsequent payments/reimbursement.

OFM may also perform financial statements and month-end and year-end financial close-outs. OFM also uses the OFM application to manage general accounting and financial operations for BEP. OFM also reviews numismatic product orders to conduct production planning activities that involve product specifications, paper type selection, order quantities, and delivery dates. OFM may also track and manage the General Ledger through MSS in addition to producing financial reports and data to Treasury. OFM may also manage BEP Office budgets, approve requisitions, and validate purchases in the OFM application. As a result, the Office of Financial Management maintains the information listed in Section 4.2 below in the OFM application to process vendor invoices and to conduct accounts payable/receivable transactions.

4) Manufacturing Inventory Application

The Office of Engraving (DCF/WCF), the Office of Currency Manufacturing (DCF/WCF), the Office of Compliance (DCF/WCF), the Office of Quality Operations (DCF/WCF), the Office of Quality Engineering and Management (WCF), the Office of Facilities Support (DCF), the Facilities Management Division (WCF), the Office of Security (DCF), the Security Division (WCF) and the Office of Environment, Health, and Safety (DCF/WCF) use the Manufacturing Inventory application for the following activities:

- Inventory management
- Manage changes to and returns of public sales orders
- Order returns management
- Tracking shipping inquiries
- Distribution and warehouse material handling management
- Item count management
- Spare part management
- Inventory adjustment and replenishment management
- Materials receiving management
- Security document count and inventory management

This application collects PII of members of the public and BEP employees and contractors. Authorized BEP employees and contractors may receive access based on their assigned duties within the currency and security document manufacturing process or associated services.

5) Manufacturing Execution Console (MEC) Application

The Office of Currency Manufacturing (DCF/WCF) use the MEC application to perform the following activities, which do not involve PII on members of the public.

- Monitoring printing press operational status
- Monitoring facility and currency production area for environmental (e.g. production area temperature and humidity monitoring), health, and safety conditions
- Interfacing with systems that manage employee facilities-related requests for services, spare parts, or materials
- Tracking of produced items and any components or ingredients used in the production process
- Work orders, work-in-progress status, job creation, and assignments
- Condition of currency/printed products reporting
- Number of products (e.g. raw materials, printed sheets) that do not conform to BEP’s quality standards
- Production planning activities for numismatic orders to manage product specifications, order quantities, and delivery dates
- Equipment performance and reliability reporting
- Hazardous materials tracking
- Equipment sensor monitoring and status reporting
- Security management for materials and inventory movement
- Maintenance management
- Product movement tracking

The MEC application contains PII from BEP employees and contractors only. To perform these activities, the MEC application interfaces with the BEP Manufacturing System, which is a separate General Support System (GSS) comprised of specialized printing presses, inspection and finishing systems, IT subsystems and components that automate process control and quality assurance. These systems provide real-time currency inspections, provide results, and control electro-mechanical actions of manufacturing equipment. The Manufacturing System does not contain PII on members of the public or BEP employees/contractors.

Estimated Number of Individuals Whose Personally Identifiable Information is Maintained in the System or by the Project		
<input type="checkbox"/> 0 – 999	<input checked="" type="checkbox"/> 1000 – 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 3.2: Authority to Collect

The authorities for operating this system or performing this project are: 5 U.S.C. § 301,¹ 31 U.S.C. § 303,² 31 U.S.C. § 3512,³ 31 U.S.C. § 5114,⁴ 44 U.S.C. § 3101,⁵ 44 U.S.C. § 2906,⁶ 44 U.S.C. § 3534⁷.

Section 4: Information Collection

Section 4.1: 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 fulfilled 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 4.1(a) Please check all of the following that are true:

1. None of the PII maintained in the system or by the project is part of a Privacy Act system of records;
2. All of the PII maintained in the system or by the project is part of a system of records and none of it is exempt from the Privacy Act relevant and necessary requirement;
3. All of the PII maintained in the system or by the project is part of a system of records and all of it is exempt from the Privacy Act relevant and necessary requirement;
4. Some, but not all, of the PII maintained in the system or by the project is part of a system of records and the records to which the Privacy Act applies are exempt from the relevant and necessary requirement; and
5. Some, but not all, of the PII maintained in the system or by the project is part of a system of records and none of the records to which the Privacy Act applies are exempt from the relevant and necessary requirement.

Section 4.1(b) Yes No N/A With respect to PII maintained in the system or by the project that is subject to the Privacy Act's relevant and necessary requirement, was an assessment conducted prior to collection (e.g., during Paperwork Reduction Act analysis) to determine which PII types (see Section 4.2 below) were relevant and necessary to meet the system's or project's mission requirements?

Section 4.1(c) Yes No N/A With respect to PII currently maintained in the system or by the project that is subject to the Privacy Act's relevant and necessary requirement, is the PII limited to only that which is relevant and necessary to meet the system's or project's mission requirements?

Section 4.1(d) Yes No With respect to PII maintained in the system or by the project that is subject to the Privacy Act's relevant and necessary requirement, is there a process to continuously reevaluate and ensure that the PII remains relevant and necessary?

BEP uses the Privacy Threshold Analysis (PTA) process to assess and limit PII collection to information that is deemed relevant and necessary in order to conduct authorized business activities. BEP also provides a continuous monitoring framework that triggers additional PTA updates each time the system or processes impacting PII are significantly altered. The BEP MSS System underwent a reassessment to determine the type of

¹ [5 U.S.C. § 301.](#)

² [31 U.S.C § 303.](#)

³ [31 U.S.C. § 3512.](#)

⁴ [31 U.S.C. § 5114.](#)

⁵ [44 U.S.C. § 3101.](#)

⁶ [44 U.S.C. § 2906.](#)

⁷ [44 U.S.C. § 3534.](#)

PII managed by the system. The reassessment allowed BEP to document additional activities conducted by various offices that use specific MSS applications.

Specifically, the Office of External Relations use the Public Sales and Manufacturing Inventory Applications to collect PII relevant and necessary to manage and fulfill public sales. BEP is amending SORN Treasury/BEP .045, Mail Order Sales Customer Files, to accurately reflect data required to fulfill orders received by email and/or telephone. The new data will include: telephone number, email address, order information (item, price, quantity, order number, order date, and order quote), currency type, customer number, and inventory data.

The Office of Financial Management and the Office of Acquisitions uses the Financial Management Application and the CLM/iProcurement Application to collect and manage PII relevant and necessary to conduct activities that include contracts/awards, the procurement process, financial accounting, and employee and vendor payment transactions. These activities receive coverage from Treasury SORN .009, Treasury Fiscal Services Systems and General Services Administration (GSA)/GOVT-4, Contracted Travel Services Program.

The Office of Engraving, the Office of Currency Manufacturing (DCF/WCF), the Office of Security (DCF), the Security Division (WCF), the Office of Compliance, the Office of Quality Operations (DCF), the Office of Quality Engineering and Management (WCF), Office of Facilities Support (DCF), the Facilities Management Division (WCF), and the Office of Environment, Health, and Safety, the Office of Acquisitions, the Office of Financial Management, and the Office of External Relations primarily use the Manufacturing Inventory Application and the Manufacturing Execution Console (MEC) Application to manage statistical or manufacturing-specific activities. With the exception of PII that is relevant and necessary to manage access accounts for BEP employees and contractors that require access to MSS applications, the remaining information is in a non-identifiable form. MSS applications receive coverage for system access and accounts from Treasury SORN .015, General Information Technology Access and Accounts Records.

Additionally, existing federal and Department of the Treasury (Treasury) systems serve as portals for external entities to conduct financial transactions, which reduces the amount and type of PII BEP requires to complete the transaction. Additionally, BEP incorporates a Risk Management Framework assessment into its PTAs to evaluate and categorize the PII confidentiality impact level (e.g. low, moderate, or high) to indicate the potential harm to individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. By migrating a substantial portion of its commercial sales activities and PII collection to the Mint, BEP minimizes the risk of collecting PII that is not relevant and necessary.

Section 4.2: PII and/or information types or groupings

To perform their various missions, federal agencies must necessarily collect various types of information. The checked boxes below represent the types of information maintained in the system or by the project. Information identified below is used by the system or project to fulfill the purpose stated in Section 3.3 – Authority to Collect.

Biographical/General Information		
<input checked="" type="checkbox"/> Name	<input checked="" type="checkbox"/> Gender	<input type="checkbox"/> Group/Organization Membership
<input checked="" type="checkbox"/> Date of Birth	<input type="checkbox"/> Race	<input type="checkbox"/> Military Service Information
<input checked="" type="checkbox"/> Home Physical/Postal Mailing Address	<input type="checkbox"/> Ethnicity	<input checked="" type="checkbox"/> Personal Home Phone or Fax Number
<input checked="" type="checkbox"/> Zip Code	<input type="checkbox"/> Personal Cell Number	<input type="checkbox"/> Alias (including nickname)
<input checked="" type="checkbox"/> Business Physical/Postal Mailing Address and Office Name	<input checked="" type="checkbox"/> Business Cell Number	<input checked="" type="checkbox"/> Business Phone or Fax Number
<input type="checkbox"/> Personal e-mail address	<input type="checkbox"/> Nationality	<input type="checkbox"/> Mother's Maiden Name
<input checked="" type="checkbox"/> Business e-mail address	<input type="checkbox"/> Country of Birth	<input type="checkbox"/> Spouse Information
<input type="checkbox"/> Personal Financial Information (including loan information)	<input type="checkbox"/> City or County of Birth	<input type="checkbox"/> Children Information

<input type="checkbox"/> Business Financial Information (including loan information)	<input type="checkbox"/> Immigration Status	<input type="checkbox"/> Information about other relatives.
<input type="checkbox"/> Marital Status	<input type="checkbox"/> Citizenship	<input type="checkbox"/> Professional/personal references or other information about an individual's friends, associates or acquaintances.
<input type="checkbox"/> Religion/Religious Preference	<input type="checkbox"/> Device settings or preferences (e.g., security level, sharing options, ringtones).	<input type="checkbox"/> Global Positioning System (GPS)/Location Data
<input type="checkbox"/> Sexual Orientation	<input type="checkbox"/> User names, avatars etc.	<input type="checkbox"/> Secure Digital (SD) Card or Other Data stored on a card or other technology
<input type="checkbox"/> Cell tower records (e.g., logs. User location, time etc.)	<input type="checkbox"/> Network communications data	<input type="checkbox"/> Cubical or office number
<input type="checkbox"/> Contact lists and directories (known to contain personal information)	<input type="checkbox"/> Contact lists and directories (not known to contain personal information, but uncertain)	<input type="checkbox"/> Contact lists and directories (known to contain only business information)
<input type="checkbox"/> Education Information	<input type="checkbox"/> Resume or curriculum vitae	<input type="checkbox"/> Other (please describe): Tested Individual's Job Title
<input checked="" type="checkbox"/> Other (please describe): Office title and location	<input type="checkbox"/> Other (please describe):	<input checked="" type="checkbox"/> Other (please describe): Employment Date

Identifying Numbers	
<input checked="" type="checkbox"/> Full Social Security number	<input type="checkbox"/> Health Plan Beneficiary Number
<input type="checkbox"/> Truncated/Partial Social Security number (e.g., last 4 digits)	<input type="checkbox"/> Alien Registration Number
<input type="checkbox"/> Personal Taxpayer Identification Number	<input checked="" type="checkbox"/> Business Taxpayer Identification Number (If known: <input type="checkbox"/> sole proprietor; <input type="checkbox"/> non-sole proprietor)
<input checked="" type="checkbox"/> Personal Credit Card Number	<input checked="" type="checkbox"/> Business Credit Card Number (If known: <input type="checkbox"/> sole proprietor; <input type="checkbox"/> non-sole proprietor)
<input type="checkbox"/> Personal Vehicle Identification Number	<input type="checkbox"/> Business Vehicle Identification Number (If known: <input type="checkbox"/> sole proprietor; <input type="checkbox"/> non-sole proprietor)
<input type="checkbox"/> Personal License Plate Number	<input type="checkbox"/> Business License Plate Number (If known: <input type="checkbox"/> sole proprietor; <input type="checkbox"/> non-sole proprietor)
<input type="checkbox"/> File/Case ID Number (individual)	<input type="checkbox"/> File/Case ID Number (business) (If known: <input type="checkbox"/> sole proprietor; <input type="checkbox"/> non-sole proprietor)
<input type="checkbox"/> Personal Professional License Number	<input type="checkbox"/> Business Professional License Number (If known: <input type="checkbox"/> sole proprietor; <input type="checkbox"/> non-sole proprietor)
<input checked="" type="checkbox"/> Employee Identification Number	<input type="checkbox"/> Patient ID Number
<input checked="" type="checkbox"/> Business Bank Account Number	<input checked="" type="checkbox"/> Personal Bank Account Number
<input type="checkbox"/> Commercially obtained internet navigation/purchasing habits of individuals	<input type="checkbox"/> Government obtained internet navigation/purchasing habits of individuals
<input type="checkbox"/> Business License Plate Number (non-sole-proprietor)	<input type="checkbox"/> Driver's License Number
<input type="checkbox"/> Personal device identifiers or serial numbers	<input checked="" type="checkbox"/> Other Identifying Numbers (please describe): CAGE and D.U.N.S. Business Entity numbers (publically available)
<input type="checkbox"/> Passport Number and Passport information (including full name, passport number, DOB, POB, sex, nationality, issuing country photograph and signature) (use "Other" if some but not all elements are collected)	<input checked="" type="checkbox"/> Other Identifying Numbers (please describe): <ul style="list-style-type: none"> • Contract numbers • Award numbers • Order numbers • Order price quote

	<ul style="list-style-type: none"> • Customer numbers • Invoice numbers • Purchase order numbers • Supplier numbers • Office/Operating Unit Number
--	---

Medical/Emergency Information Regarding Individuals		
<input type="checkbox"/> Medical/Health Information	<input type="checkbox"/> Worker's Compensation Act Information	<input type="checkbox"/> Patient ID Number
<input type="checkbox"/> Mental Health Information	<input type="checkbox"/> Disability Information	<input type="checkbox"/> Emergency Contact Information (e.g., a third party to contact in case of emergency)
<input type="checkbox"/> Other (please describe):		

Biometrics/Distinguishing Features/Characteristics of Individuals		
<input type="checkbox"/> Physical description/ characteristics (e.g., hair, eye color, weight, height, sex, gender etc.)	<input checked="" type="checkbox"/> Signatures (including digital)	<input type="checkbox"/> Vascular scans
<input type="checkbox"/> Fingerprints	<input type="checkbox"/> Photos	<input type="checkbox"/> Retina/Iris Scans
<input type="checkbox"/> Palm prints	<input type="checkbox"/> Video	<input type="checkbox"/> Dental Profile
<input type="checkbox"/> Voice audio recording	<input type="checkbox"/> Scars, marks, tattoos	<input type="checkbox"/> DNA Sample or Profile
<input type="checkbox"/> Other (please describe):	<input type="checkbox"/> Other (please describe):	<input type="checkbox"/> Other (please describe):

Specific Information/File Types		
<input type="checkbox"/> Taxpayer Information/Tax Return Information	<input type="checkbox"/> Law Enforcement Information	<input type="checkbox"/> Security Clearance/Background Check Information
<input type="checkbox"/> Civil/Criminal History Information/Police Records (government source)	<input type="checkbox"/> Credit History Information (government source)	<input type="checkbox"/> Bank Secrecy Act Information
<input type="checkbox"/> Civil/Criminal History Information/Police Records (commercial source)	<input type="checkbox"/> Credit History Information (commercial source)	<input type="checkbox"/> National Security/Classified Information
<input type="checkbox"/> Protected Information (as defined in Treasury Directive 25-10)	<input type="checkbox"/> Case files	<input type="checkbox"/> Personnel Files
<input type="checkbox"/> Information provided under a confidentiality agreement	<input type="checkbox"/> Information subject to the terms of an international or other agreement	<input checked="" type="checkbox"/> Other (please describe): <ul style="list-style-type: none"> • Employee financial payments/reimbursements and payment information (e.g. Travel and Personal Property Claims) • Invoice date • Invoice approval status • Invoice amount • Payment date • Payment Currency (e.g. USD) • Payment amount (partial, remaining, and/or total amount) • Payment Type (e.g. EFT, Check) • Supplier number

		<ul style="list-style-type: none"> • Statistical data on BEP procurements and/or contracts • History of customer sales • Order itemOrder quantity
--	--	--

Audit Log and Security Monitoring Information		
<input checked="" type="checkbox"/> User ID assigned to or generated by a user of Treasury IT	<input checked="" type="checkbox"/> Date and time an individual accesses a facility, system, or other IT	<input type="checkbox"/> Files accessed by a user of Treasury IT (e.g., web navigation habits)
<input checked="" 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"/> Biometric information used to access Treasury facilities or IT	<input type="checkbox"/> Video of individuals derived from security cameras	<input type="checkbox"/> Public Key Information (PKI).
<input 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 or devices	<input type="checkbox"/> Still photos of individuals derived from security cameras.	<input checked="" type="checkbox"/> Internet Protocol (IP) Address
<input checked="" type="checkbox"/> Other (please describe): Metadata/user access statistical data.	<input checked="" type="checkbox"/> Other (please describe): Access group name.	<input type="checkbox"/> Other (please describe): _____

Other	
<input type="checkbox"/> Other (please describe: _____	<input type="checkbox"/> Other (please describe: _____
<input type="checkbox"/> Other (please describe: _____	<input type="checkbox"/> Other (please describe: _____

Data Collection by Specific MSS Applications

1) CLM/iProcurement Application:

- Vendor/Business Name
- Point of Contact Name
- Business Address
- Ship to Location/Address
- Business Phone Number
- Business Email Address
- Tax Identification Number (Tax ID)
- CAGE Code (5-digit) – *GSA System Award Management Publically Available*
- Public Dun & Bradstreet Business ID Number (D-U-N-S Number) (9-digit) - *Publically Available*
- Award Number

2) Public Sales Application:

- Name of Purchaser/Customer (e.g. Individual and/or Company)
- Mailing Address
- Telephone number
- Email address

- Order information (item, price, quantity, order quote, order number, and order date)
- Currency type (e.g. USD)
- Customer/purchaser number
- History of customer sales
- Credit Card Information – For purchases made in-person in the BEP store, the BEP will process the credit card information through the BFS CAS System and will not store it in the Public Sales application. The last 4 digits of the credit card number will be printed on the receipt of sale. For all other purchases, BEP will collect the information by phone and also process the payment manually through the BFS CAS System or direct bulk purchasers that require electronic (wire) transactions to the BFS CIR System.

3) Office of Financial Management Application:

- Payee/Trading Partner/Supplier Name
- Payee/Trading Partner/Supplier banking information
- SSN/Tax ID number
- Employee ID Number
- Invoice number
- Invoice date
- Invoice approval status
- Invoice amount
- Purchase order number
- Payment date
- Payment Currency (e.g. USD)
- Payment amount (partial, remaining, and/or total amount)
- Payment Type (e.g. EFT, Check)
- Supplier number

BEP maintains the following information on BEP employees in order to facilitate non pay-roll related financial payments or reimbursements:

- Employee name
- Social Security number (SSN)/Tax ID number
- Employee ID number
- Electronic Funds Transaction (EFT) banking information (account and routing number)
- Title
- Date of birth
- Gender
- Business email address
- Business telephone number
- Employment date
- Payment date
- Payment Currency (e.g. USD)
- Payment amount (partial, remaining, and/or total amount)
- Payment Type (e.g. EFT, Check (if check is the authorized payment method))
- Payment Address (if applicable)

4) Manufacturing Inventory Application:

- Name of Purchaser/Customer (e.g. Individual and/or Entity)
- Mailing Address
- Order information (item, price, quantity, order number, order quote, and order date)

It also includes the following PII for BEP employees and contractors that maintain customer data:

- Employee/contractor name
- Office title and location
- Office/work telephone number
- User Name/Login
- Password
- IP Address
- Access Group Name
- Metadata/User Access Statistical Information

5) Manufacturing Execution Console (MEC) Applications (This application does not contain PII on members of the public):

- Employee/contractor name
- Office title and location
- Office/work telephone number
- User Name/Login
- Password
- IP Address
- Access Group Name
- Metadata/User Access Statistical Information

Section 4.3: Sources of information and the method and manner of collection

CLM/iProcurement Application	Public Sales Application	Office of Financial Management Application	MSS Users/System Administrators
-------------------------------------	---------------------------------	---	--

<p>Specific PII identified in Section 4.2 acquired from this source:</p> <ul style="list-style-type: none"> • Vendor/Supplier/Business Name • Point of Contact Name • Business Address • Ship to/Bill to Location/Address • Business Phone Number • Business Email Address • Tax Identification Number (Tax ID) • CAGE Code (5-digit) - <i>Publically Available</i> • Dun & Bradstreet Business ID Number (D-U-N-S Number) (9-digit) <i>Publically Available</i> • Trading partner/payee Name • Trading partner/payee bank account information • Invoice number • Invoice date • Invoice approval status • Invoice amount • Purchase order number • Payment date • Payment Currency (e.g. USD) • Payment amount (partial, remaining, and/or total amount) • Payment Type (e.g. EFT, Check) • Supplier number • Date ordered • Order number • Order type • Statistical data 	<p>Specific PII identified in Section 4.2 acquired from this source:</p> <ul style="list-style-type: none"> • Name of Purchaser/Customer (e.g. Individual and/or Company) • Mailing Address • Credit Card Information • Order information: <ul style="list-style-type: none"> ○ Item ○ Price ○ Quantity ○ Order number ○ Order quote ○ Order date • Payment Currency (e.g. USD) • Customer/purchaser number • History of customer sales <p>(Credit Card information is not stored in MSS)</p>	<p>Specific PII identified in Section 4.2 acquired from this source:</p> <ul style="list-style-type: none"> • Employee Name • SSN/Tax ID Number • Employee ID Number • Electronic Funds Transaction (EFT) Banking Information (Account and Routing number) • Date of birth • Gender • Business email address • Business telephone number • Employment date • Payment date • Payment Currency (e.g. USD) • Payment amount (partial, remaining, and/or total amount) • Payment Type (e.g. EFT, Check) • Payment Address (if applicable) 	<p>Specific PII identified in Section 4.2 acquired from this source:</p> <ul style="list-style-type: none"> • User Name/Login • Office Title/Office Location • Password • IP Address • Access Group Name • Metadata/User Access Statistical Information
<p>Manner in which information is acquired from source by the Treasury project/system: (select all that apply):</p>	<p>Manner in which information is acquired from source by the Treasury project/system: (select all that apply):</p>	<p>Manner in which information is acquired from source by the Treasury project/system: (select all that apply):</p>	<p>Manner in which information is acquired from source by the Treasury project/system: (select all that apply):</p>
<p><input type="checkbox"/> From a paper or electronic form provided to individuals, the public or members of a particular group</p>	<p><input type="checkbox"/> From a paper or electronic form provided to individuals, the public or members of a particular group</p>	<p><input checked="" type="checkbox"/> From a paper or electronic form provided to individuals, the public or members of a particular group</p>	<p><input type="checkbox"/> From a paper or electronic form provided to individuals, the public or members of a particular group</p>

Please identify the form name (or description) and/or number (e.g., OMB Control Number): Solicitation of Proposal Information for Award of Contract – OMB Control Number 1505-0081 and Post-Contract Award Information -1505-0080 _____	Please identify the form name (or description) and/or number (e.g., OMB Control Number): _____	Please identify the form name (or description) and/or number (e.g., OMB Control Number): SF-1164 –Claim for Reimbursement for Expenditures on Official Business	Please identify the form name (or description) and/or number (e.g., OMB Control Number): _____
<input checked="" type="checkbox"/> Received in paper format other than a form.	<input checked="" type="checkbox"/> Received in paper format other than a form.	<input type="checkbox"/> Received in paper format other than a form.	<input type="checkbox"/> Received in paper format other than a form.
<input type="checkbox"/> Delivered to the project on disk or other portable device and uploaded to the system.	<input type="checkbox"/> Delivered to the project on disk or other portable device and uploaded to the system.	<input type="checkbox"/> Delivered to the project on disk or other portable device and uploaded to the system.	<input type="checkbox"/> Delivered to the project on disk or other portable device and uploaded to the system.
<input checked="" type="checkbox"/> Accessed and downloaded or otherwise acquired via the internet	<input type="checkbox"/> Accessed and downloaded or otherwise acquired via the internet	<input type="checkbox"/> Accessed and downloaded or otherwise acquired via the internet	<input type="checkbox"/> Accessed and downloaded or otherwise acquired via the internet
<input checked="" type="checkbox"/> Email	<input checked="" type="checkbox"/> Email (No credit card information)	<input type="checkbox"/> Email	<input type="checkbox"/> Email
<input type="checkbox"/> Scanned documents uploaded to the system.	<input type="checkbox"/> Scanned documents uploaded to the system.	<input type="checkbox"/> Scanned documents uploaded to the system.	<input type="checkbox"/> Scanned documents uploaded to the system.
<input type="checkbox"/> Bulk transfer	<input type="checkbox"/> Bulk transfer	<input type="checkbox"/> Bulk transfer	<input type="checkbox"/> Bulk transfer
<input type="checkbox"/> Extracted from particular technology (e.g., radio frequency identification data (RFID) devices, video or photographic cameras, biometric collection devices):	<input type="checkbox"/> Extracted from particular technology (e.g., radio frequency identification data (RFID) devices, video or photographic cameras, biometric collection devices):	<input type="checkbox"/> Extracted from particular technology (e.g., radio frequency identification data (RFID) devices, video or photographic cameras, biometric collection devices):	<input type="checkbox"/> Extracted from particular technology (e.g., radio frequency identification data (RFID) devices, video or photographic cameras, biometric collection devices):
<input type="checkbox"/> Fax	<input type="checkbox"/> Fax	<input type="checkbox"/> Fax	<input type="checkbox"/> Fax
<input checked="" type="checkbox"/> Extracted from notes of a phone interview or face to face contact	<input checked="" type="checkbox"/> Extracted from notes of a phone interview or face to face contact	<input type="checkbox"/> Extracted from notes of a phone interview or face to face contact	<input type="checkbox"/> Extracted from notes of a phone interview or face to face contact
<input checked="" type="checkbox"/> Other: Please describe: Electronic invoices, purchase orders, and procurement and contract solicitation documents submitted to BFS CIR.	<input checked="" type="checkbox"/> Other: Please describe: Postal/Mail Order	<input checked="" type="checkbox"/> Other: Please describe: OFM/BFS FMS interface to verify identify and EFT banking information through the NFC.	<input checked="" type="checkbox"/> Other: Please describe: Network/System Accounts/Computer Name
<input type="checkbox"/> Other: Please describe:	<input type="checkbox"/> Other: Please describe: _____	<input type="checkbox"/> Other: Please describe: _____	<input type="checkbox"/> Other: Please describe: _____
Manufacturing Inventory Application	Manufacturing Execution Console Application		

<p>Specific PII identified in Section 4.2 acquired from this source:</p> <ul style="list-style-type: none"> • Name of Purchaser/Customer (e.g. Individual and/or Company) • Mailing Address • Order information: <ul style="list-style-type: none"> ○ Item ○ Price ○ Quantity ○ Order number ○ Order quote 	<p>Specific PII identified in Section 4.2 acquired from this source:</p> <ul style="list-style-type: none"> • Employee/contractor name • Office title and location • Office/work telephone number • User Name/Login • Password • IP Address • Access Group Name • Metadata/User Access Statistical Information 		
<p>Manner in which information is acquired from source by the Treasury project/system: (select all that apply):</p>	<p>Manner in which information is acquired from source by the Treasury project/system: (select all that apply):</p>	<p>Manner in which information is acquired from source by the Treasury project/system: (select all that apply):</p>	<p>Manner in which information is acquired from source by the Treasury project/system: (select all that apply):</p>
<p><input type="checkbox"/> From a paper or electronic form provided to individuals, the public or members of a particular group</p>	<p><input type="checkbox"/> From a paper or electronic form provided to individuals, the public or members of a particular group</p>	<p><input type="checkbox"/> From a paper or electronic form provided to individuals, the public or members of a particular group</p>	<p><input type="checkbox"/> From a paper or electronic form provided to individuals, the public or members of a particular group</p>
<p>Please identify the form name (or description) and/or number (e.g., OMB Control Number): _____</p>	<p>Please identify the form name (or description) and/or number (e.g., OMB Control Number): _____</p>	<p>Please identify the form name (or description) and/or number (e.g., OMB Control Number): _____</p>	<p>Please identify the form name (or description) and/or number (e.g., OMB Control Number): _____</p>
<p><input checked="" type="checkbox"/> Received in paper format other than a form.</p>	<p><input type="checkbox"/> Received in paper format other than a form.</p>	<p><input type="checkbox"/> Received in paper format other than a form.</p>	<p><input type="checkbox"/> Received in paper format other than a form.</p>
<p><input type="checkbox"/> Delivered to the project on disk or other portable device and uploaded to the system.</p>	<p><input type="checkbox"/> Delivered to the project on disk or other portable device and uploaded to the system.</p>	<p><input type="checkbox"/> Delivered to the project on disk or other portable device and uploaded to the system.</p>	<p><input type="checkbox"/> Delivered to the project on disk or other portable device and uploaded to the system.</p>
<p><input type="checkbox"/> Accessed and downloaded or otherwise acquired via the internet</p>	<p><input type="checkbox"/> Accessed and downloaded or otherwise acquired via the internet</p>	<p><input type="checkbox"/> Accessed and downloaded or otherwise acquired via the internet</p>	<p><input type="checkbox"/> Accessed and downloaded or otherwise acquired via the internet</p>
<p><input checked="" type="checkbox"/> Email</p>	<p><input type="checkbox"/> Email (No credit card information)</p>	<p><input type="checkbox"/> Email</p>	<p><input type="checkbox"/> Email</p>
<p><input type="checkbox"/> Scanned documents uploaded to the system.</p>	<p><input type="checkbox"/> Scanned documents uploaded to the system.</p>	<p><input type="checkbox"/> Scanned documents uploaded to the system.</p>	<p><input type="checkbox"/> Scanned documents uploaded to the system.</p>
<p><input type="checkbox"/> Bulk transfer</p>	<p><input type="checkbox"/> Bulk transfer</p>	<p><input type="checkbox"/> Bulk transfer</p>	<p><input type="checkbox"/> Bulk transfer</p>
<p><input type="checkbox"/> Extracted from particular technology (e.g., radio frequency identification data (RFID) devices, video or</p>	<p><input type="checkbox"/> Extracted from particular technology (e.g., radio frequency identification data (RFID) devices, video or photographic cameras,</p>	<p><input type="checkbox"/> Extracted from particular technology (e.g., radio frequency identification data (RFID) devices, video or</p>	<p><input type="checkbox"/> Extracted from particular technology (e.g., radio frequency identification data (RFID) devices, video or</p>

photographic cameras, biometric collection devices):	biometric collection devices):	photographic cameras, biometric collection devices):	photographic cameras, biometric collection devices):
<input type="checkbox"/> Fax	<input type="checkbox"/> Fax	<input type="checkbox"/> Fax	<input type="checkbox"/> Fax
<input type="checkbox"/> Extracted from notes of a phone interview or face to face contact	<input type="checkbox"/> Extracted from notes of a phone interview or face to face contact	<input type="checkbox"/> Extracted from notes of a phone interview or face to face contact	<input type="checkbox"/> Extracted from notes of a phone interview or face to face contact
<input checked="" type="checkbox"/> Other: Please describe:	<input checked="" type="checkbox"/> Other: Please describe: Network/System Account/ Computer Name	<input type="checkbox"/> Other: Please describe:	<input type="checkbox"/> Other: Please describe:
<input checked="" type="checkbox"/> Other: Please describe: In addition to email, postal mail and telephone orders and added to the application by OEX personnel to manage inventory.	<input type="checkbox"/> Other: Please describe: _____	<input type="checkbox"/> Other: Please describe: _____	<input type="checkbox"/> Other: Please describe: _____

Section 4.4: Privacy and/or civil liberties risks related to collection

Notice of Authority, Principal Uses, Routine Uses, and Effect of not Providing Information

When Federal agencies use a form to obtain 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 her/him, if any, of not providing all or any part of the requested information.” 5 U.S.C § 522a(e)(3).

Section 4.4(a) Yes No Is any of the PII maintained in the system or by the project collected directly from an individual?

Section 4.4(b) Yes No N/A Was the information collected from the individual using a form (paper or electronic)?

Section 4.4(c) Yes No N/A If the answer to Section 4.4(b) was “yes,” was the individual notified (on the form in which the PII was collected or on a separate form that can be retained by the individual) about the following at the point where the information was collected (e.g., in a form; on a website).

- The authority (whether granted by statute, or by Executive order of the President) which authorizes the solicitation of the information.
- Whether disclosure of such information is mandatory or voluntary.
- The principal purpose or purposes for which the information is intended to be used.
- The individuals or organizations outside of Treasury with whom the information may be/ will be shared.

<input checked="" type="checkbox"/> The effects on the individual, if any, if they decide not to provide all or any part of the requested information.
<p>Business entities that submit Acquisitions/Procurement information through the BFS CIR System will receive a BFS Privacy Act notice posted on the BFS Internet Portal prior to the information arriving BEP through the CLM/iProcurement Application.</p> <p>Numismatic and engraved product purchasers that submit information to OEX will receive written Privacy Act notice at the point of sale for in-person purchases, verbally during phone-in orders, or by email. OEX's performed the Privacy Act compatibility assessment with respect to the disclosure of a record outside of Treasury (i.e., external sharing) and no new routines uses were identified. Please see Attachment I of the PCLIA.</p> <p>BEP employees scheduled to receive non-payroll payments will receive Privacy Act notice included on the Claim for Reimbursement for Expenditures on Official Business Form (SF-1164).</p> <p>PII managed in the Manufacturing Inventory Application originates from information provided to OEX during the public sales process. Individuals will receive notice directly from OEX. There are no PII data collections pertaining to the Manufacturing Execution Console (MEC) Application.</p>

Use of Social Security Numbers

Social Security numbers (“SSN”) are commonly used by identity thieves to commit fraudulent acts against individuals. The SSN is one data element that has the ability to harm the individual and requires more protection when used. Therefore, and in an effort to reduce risk to individuals and federal agencies, OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, (May 22, 2007) required agencies to reduce the use of SSNs in agency systems and programs and to identify instances in which the collection is superfluous. In addition, OMB mandated agencies to explore alternatives to agency use of SSNs as personal identifiers for Federal employees and members of the public.

In addition, 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).

<p>Section 4.4(d) <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A Does the system or project maintain SSNs?</p> <p>Section 4.4(e) <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A Are there any alternatives to the SSNs as a personal identifier? If yes, please provide a narrative explaining why other alternatives to identify individuals will not be used.</p> <p>Section 4.4(f) <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> N/A Will individuals be denied any right, benefit, or privilege provided by law because of such individual’s refusal to disclose their SSN? If yes, please check the applicable box::</p> <p style="margin-left: 40px;"> <input type="checkbox"/> SSN disclosure is required by Federal statute or Executive Order. ; or <input type="checkbox"/> the SSN is disclosed to any Federal, state, or local agency maintaining a <u>system of records</u> 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. <i>If checked, please provide the name of the system of records in the space provided below:</i> </p>
--

Section 4.4(g) Yes No N/A When the SSN is collected, are individuals given notice whether disclosure is mandatory or voluntary, the legal authority such number is solicited, and what uses will be made of it? If yes, please explain what means are used to provide notice.

The Office of Financial Management Application uses the SSN of employees to verify identity prior to direct non-payroll payment/reimbursements of travel and personal property claims. BEP queries the NFC through BFS FMS to verify the identity of the employee and obtain their EFT/banking information through data previously maintained by the NFC in order to process the payment. The OFM Payment Processor then creates a payee/supplier record using the Employee ID Number, EFT/Banking information, contact information, and agency financial account data to process the payment/reimbursement. The Employee ID Number is static and alleviates the need to verify the employee's SSN for subsequent claim submissions. BEP further mitigates risks by limiting the information to individuals that have a need for the information and through secure data transmission within the Treasury network to BFS for payment processing.

The Office of Financial Management Application and the CLM/iProcurement Application also contains SSNs or Tax ID numbers of individuals or business entities conducting financial transactions with BEP. Business entities may provide their Tax ID numbers associated with their business/corporate account to the BFS and Office of Acquisitions. In many instances, Tax ID numbers are publicly available.

There are no SSN or Tax ID Number collections pertaining to the Manufacturing Inventory Application, Public Sales Application, or the Manufacturing Execution Console (MEC).

First Amendment Activities

The Privacy Act provides 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(b)(7).

Section 4.4(h) Yes No Does the system or project maintain any information describing how an individual exercises their rights guaranteed by the First Amendment?

Section 4.4(i) If the system or project maintains information describing how an individual exercises their rights guaranteed by the First Amendment, do any of the following exceptions apply (the information may be maintained if any of the exceptions apply)?

N/A (system or project does not maintain any information describing how an individual exercises their rights guaranteed by the First Amendment so no exceptions are needed)

- The individual about whom the information was collected or maintained expressly authorizes its collection/maintenance.
- The information maintained is pertinent to and within the scope of an authorized law enforcement activity.
- There is a statute that expressly authorizes its collection.
- N/A, the system or project does not maintain any information describing how any individual exercises their rights guaranteed by the First Amendment.

N/A These parameters apply to all applications under MSS.

Section 5: Maintenance, use, and sharing of the information

The following sections require a clear description of the system's or project's use of information.

Section 5.1: Describe how and why the system or project uses the information it collects and maintains

Please describe all of the uses of the information types and groupings collected and maintained by the system or project (see Section 4.2), including a discussion of why the information is used for this purpose and how it relates to the mission of the bureau or office that owns the system.

The Office of Financial Management and the Office of Acquisitions uses PII to manage financial activities in Financial Management Application and the CLM/iProcurement Application to support individuals and entities conducting business with or purchasing numismatic products from BEP and to process non-payroll related financial payments/reimbursements to BEP employees. They also manage accounts payable/receivable transactions between business entities/vendors/suppliers, and to meet non-PII related budgetary requirements.

OEX use the Manufacturing Inventory Application to store statistical data to determine the success of certain products and whether it should replenish inventory maintained at BEP and the U.S. Mint that sells numismatic products on BEP’s behalf.

The Office of Engraving, the Office of Currency Manufacturing (DCF/WCF), the Office of Security (DCF), the Security Division (WCF), the Office of Compliance, the Office of Quality Operations (DCF), the Office of Quality Engineering and Management (WCF), Office of Facilities Support (DCF), the Facilities Management Division (WCF), and the Office of Environment, Health, and Safety, the Office of Acquisitions, the Office of Financial Management, and the Office of External Relations uses the Manufacturing Inventory Application and the Manufacturing Executions Console (MSC) to manage currency and printed product manufacturing activities related to facilities, equipment, product quality, environmental and physical safety matters, maintenance, and inventory activities. These additional activities do not raise additional privacy risks because they do not involve PII collection with the exception of system user data such as login/password information, meta-data, and statistical data to manage accounts and access to the system.

Overall, MSS supports these activities by allowing BEP to leverage a single system to manage contracts/awards, manage suppliers, create and process requisitions, enter purchase orders, manage inventory, vendor records, and deliverables. These activities allow BEP to perform and manage its required duties to provide numismatic products to individuals and entities on behalf of the Federal government.

Collecting Information Directly from the Individual When Using it to Make Adverse Determinations About Them

The Privacy Act requires that Federal agencies “collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual’s rights, benefits, and privileges under Federal programs.” 5 U.S.C. § 552a(e)(2).

Section 5.1(a) Yes No Is it possible that the information maintained in the system or by the project may be used by Treasury to make an adverse determination about an individual’s rights, benefits, and privileges under federal programs (e.g., decisions about whether the individual will receive a financial benefit, get a clearance or access to a Treasury facility, obtain employment with Treasury)?

Section 5.1(b) Yes No Is it possible that Treasury will share information maintained in the system or by the project with a third party external to the Department that will use the information to make an adverse determination about an individual’s rights, benefits, and privileges under federal programs?

Section 5.1(c) Yes No N/A If information could potentially be used to make an adverse determination about an individual’s rights, benefits, and privileges under federal programs, does the system or project collect information (to the greatest extent practicable) directly from the individual?

See Section 5.2(f) below.

Data Mining

As required by Section 804 of the Implementing the 9/11 Commission Recommendations 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 reports available at: <http://www.treasury.gov/privacy/annual-reports>.

Section 5.1(d) Yes No Is information maintained in the system or by the project used to conduct “data-mining” activities as that term is defined in the Implementing the 9-11 Commission Act?

N/A. These parameters apply to all applications under MSS.

Section 5.2: Ensuring accuracy, completeness, and timeliness of information collected, maintained, and shared

Exemption from Accuracy, Relevance, Timeliness, and Completeness Requirements

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 2 above), an agency may exempt the system of records (or a portion of the records) from this requirement.

Section 5.2(a) Yes No Is all or any portion of the information maintained in the system or by the project: (a) part of a system of records and (b) exempt from the accuracy, relevance, timeliness, and completeness requirements in sections (e)(5) of the Privacy Act?

There are no exemptions claimed for the following System of Records Notices: Treasury/BEP .045 – Mail Order Sales Customer Files; Treasury .009 – Treasury Fiscal Service Systems; Treasury .015 - General Information Technology Access Account Records; and GSA/GOVT-4 - Contracted Travel Services Program.

Computer Matching

The Computer Matching and Privacy Protection Act of 1988 amended the Privacy Act imposing additional requirements when Privacy Act systems of records are used in computer matching programs.

Pursuant to the Privacy Act, as amended, 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 and recipient agencies. The matching agreement describes the purpose and procedures of the matching **and** establishes protections for matching records.

Section 5.2(b) Yes No Is any of the information maintained in the system or by the project (a) part of a system of records and (b) used as part of a matching program?

Section 5.2(c) Yes No N/A Is there a matching agreement in place that contains the information required by Section (o) of the Privacy Act?

Section 5.2(d) Yes No N/A Are assessments made regarding the accuracy of the records that will be used in the matching program?

Section 5.2(e) Yes No N/A Does the bureau or office that owns the system or project independently verify the information, provide the individual notice and an opportunity to contest the findings, or obtain Data Integrity Board approval in accordance with Section (p) of the Privacy Act before taking adverse action against the individual?

N/A. These parameters apply to all applications under MSS.

Ensuring Fairness in Making Adverse Determinations About Individuals

Federal agencies are required to “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). This requirement also applies when merging records from two or more sources where the merged records are used by the agency to make any determination about any individual.

Section 5.2(f) Yes No With respect to the information maintained in the system or by the project, are steps taken to ensure all information used to make a determination about an individual is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination?

Whenever possible, BEP collects information directly from the subject individual. Individuals conducting procurement or financial activities with BEP and providing information contained in the CLM/iProcurement and Office of Financial Management Applications may provide information initially to the BFS prior to the data arriving BEP for review. Information submitted to BFS and evaluated by BEP upon receipt could result in adverse determinations that may prevent individuals or entities from conducting business with or procuring products from BEP when procurement or financial practices reveal the violation or potential violation of civil, administrative, or criminal law, or regulations may have occurred. Additionally, adverse determinations could be made as a result of violations, potential violations, or fraud and abuse against the Federal government during procurement or financial activities.

Individuals that submit information stored in the Public Sales Application and the Manufacturing Inventory Application may also be prohibited from conducting purchases of numismatic or engraved products as a result of adverse determinations associated with fraudulent activity associated with credit card purchases.

BEP minimizes any potential risks regarding accuracy, relevance, timeliness, and completeness of records by collecting the information directly from the individual/business entity or from federal Internet portals where the individual entered financial data. The individual/entity maintains the ability to review and correct their information at the time of initial or subsequent submission. Collecting minimal PII for BEP uses further

minimizes BEP's risk of sharing inaccurate information that could be used to make determinations about an individual.

BEP manufacturing activities do not subject individuals to adverse determinations about their rights, benefits, and privileges under federal programs.

Merging Information About Individuals

Section 5.2(g) Yes No Is information maintained in the system or by the project merged with electronic or non-electronic information from internal or external sources (e.g., other files or systems)?

Section 5.2(h) Yes No N/A Once merged, is the information used in making determinations about individuals (e.g., decisions about whether the individual will receive a financial benefit or payment, get a clearance or access to a Treasury facility, obtain employment with Treasury, etc.)?

Section 5.2(i) Yes No N/A Are there documented policies or procedures for how information is merged?

Section 5.2(j) Yes No N/A Do the documented policies or procedures address how to proceed when partial matches (where some, but not all of the information being merged matches a particular individual) are discovered after the information is merged?

Section 5.2(k) Yes No N/A If information maintained in the system or by the project is used to make a determination about an individual, are steps taken to ensure the accuracy, relevance, timeliness, and completeness of the information as is reasonably necessary to assure fairness to the individual?

5.2.(g): The CLM/iProcurement and Office of Financial Management Applications receives PII or information from the BFS CIR System collected from business entities that submit information to Pay.gov The information is merged with information gathered by OA during the procurement, contract award, and/or the accounts payable/receivable processes. OFM may receive PII or information from the NFC through the BFS FMS system pertaining to personnel non-payroll payments and reimbursements. The Public Sales Application and the Manufacturing Inventory Application may receive PII or information from BFS CAS following credit card payments for numismatic products. The Manufacturing Execution Console Application may receive system access and account information associated with BEP personnel activities. No additional PII is merged with MSS applications.

5.2.(h): The CLM/iProcurement and Office of Financial Management Applications involve data transmitted to BEP from BFS. Information submitted to BFS and evaluated by BEP upon receipt could result in adverse determinations that may prevent individuals or entities from conducting business with or procuring products from BEP when procurement or financial practices reveal the violation or potential violation of civil, administrative, or criminal law, or regulations may have occurred. Additionally, adverse determinations could be made as a result of violations, potential violations, or fraud and abuse against the Federal government during procurement or financial activities. Individuals that submit information stored in the Public Sales Application and the Manufacturing Inventory Application may also be prohibited from conducting purchases of numismatic or engraved products as a result of adverse determinations associated with fraudulent activity associated with credit card purchases. BEP manufacturing activities do not subject individuals to adverse determinations about their rights, benefits, and privileges under federal programs.

5.2.(i): BEP financial activities are governed by Department of the Treasury policies and procedures promulgated in the Treasury Financial Manual (TD 16-11) and Department of the Treasury Acquisition Procedures (DTAP). These policies direct BEP to use BFS financial systems and processes that ultimately share PII related to individuals or entities conducting business with BEP or personnel authorized non-payroll payments or reimbursements.

5.2.(j): Information received from BFS in support of financial and/or procurement activities (e.g. CLM/iProcurement and Office of Financial Management Applications) is deemed accurate because it originates from the individual or business entity's submission to BFS CIR System. BFS transmits information directly to Office of Financial Management and CLM/iProcurement Applications and accounts associated with the individual

or business entity. BFS CAS does not transmit PII pertaining to an individual or business entity other than declined purchases/transactions. There is no information merged from external or internal entities with the Manufacturing Execution Console (MEC) or Manufacturing Inventory Applications.

5.2(k): BEP minimizes potential risks regarding accuracy, relevance, timeliness, and completeness of records by collecting the information directly from the individual/business entity or from federal Internet portals where the individual entered financial data. The individual/entity maintains the ability to review and correct their information at the time of initial or subsequent submission. Collecting minimal PII for BEP uses further minimizes BEP's risk of sharing inaccurate information that could be used to make determinations about an individual. These parameters apply to all MSS applications.

Policies and Standard Operating Procedures or Technical Solutions Designed to Ensure Information Accuracy, Completeness, and Timeliness

Section 5.2(l) Yes No N/A If information maintained in the system or by the project is used to make any determination about an individual (even if it is an exempt system of records), are there documented policies or standard operating procedures for the system or project that address the accuracy, completeness, and timeliness of the information?

Section 5.2(m) Yes No Does the system or project use any software or other technical solutions designed to improve the accuracy, completeness, and timeliness of the information used to make an adverse determination about an individual's rights, benefits, and/or privileges (regardless of if it is an exempt system of records)?

BEP uses the PTA review process to access systems, applications, and information collection initiatives to ensure data accuracy, completeness, and timeliness for all MSS applications. This assessment becomes part of the Federal Information Security Modernization Act (FISMA) annual review process.

The Public Sales, CLM/iProcurement, and Office of Financial Management Applications receive source information from BFS CIR. Individuals and business entities may review and/or update their information at the time of entry into the federal Internet portals that manage their financial data or at the time of purchase of numismatic or printed products or at their discretion. They may also seek to access and or correct records pursuant to the Privacy Act. The CLM/iProcurement and Office of Financial Management Applications receive automatic updates from BFS, which receives similar updates from source systems such as Pay.Gov. The automated updates allow BEP to use and maintain current information, which reduces the risk of making adverse determinations from inaccurate or obsolete data.

The Manufacturing Inventory Application data is entered by BEP personnel and is not subject to direct correction by individuals or business entities. BEP does not maintain data in the Manufacturing Execution Console in an identifiable form.

Accuracy, Completeness, and Timeliness of Information Received from the Source

Section 5.2(n) Yes No Did Treasury or the bureau receive any guarantee, assurance, or other information from any information source(s) regarding the accuracy, timeliness and completeness of the information maintained in the system or by the project?

Since BEP collects PII directly from the individual to whom it pertains, from federal systems where the individual provided the information, or from established federal employee financial systems, BEP deems this information accurate. Individuals reserve the right to correct their information with the entity that originally obtained the information.

Disseminating Notice of Corrections of or Amendments to PII

Section 5.2(o) Yes No N/A Where feasible and appropriate, is there a process in place for disseminating corrections of or amendments to the PII maintained in the system or by the project to all internal and external information-sharing partners?

Section 5.2(p) Yes No N/A Where feasible and appropriate, does the process for disseminating corrections or amendments include notifying the individual whose information is corrected or amended?

The information contained in this system originates from the individual and involves their financial information used to facilitate business transactions or numismatic, printed or engraved product purchases. BEP will not alter such information arbitrarily unless directed to do so by the individual through a Privacy Act request.

Section 5.3: Information sharing within the Department of the Treasury

Internal Information Sharing

Section 5.3(a) Yes No N/A Is PII maintained in the system or by the project shared with other Treasury bureaus?

Section 5.3(b) Yes No N/A Does the Treasury bureau or office that receives the PII limit access to those Treasury officers and employees who have a need for the PII in the performance of their official duties (i.e., those who have a “need to know”)?

BEP shares Acquisition/Procurement Management information in its CLM/iProcurement Application with BFS to facilitate contracting/acquisition processes.

BEP shares Commercial/Public Sales PII with the U.S. Mint as part of a joint program to sale numismatic, printed, or engraved products to purchasers.

BEP shares PII with BFS for processing by the NFC to facilitate non-payroll related payments to BEP employees and contractors.

BEP may share user account PII of BEP personnel within the Department of the Treasury to manage access to other Treasury and/or Bureau systems or applications. .

Memorandum of Understanding/Other Agreements Limiting Treasury’s Internal Use/Disclosure of PII

Section 5.3(c) Yes No N/A Is any of the PII maintained in the system or by the project subject to the requirements of a Memorandum of Understanding or other agreement (e.g., agreement with another federal or state agency that provided the information to the Treasury or subject to an international agreement or treaty) that limits or places conditions on Treasury’s internal use, maintenance, handling, or disclosure of the PII?

N/A. These parameters apply to all applications under MSS.

Internal Information Sharing Chart

Internal Recipient’s Name (e.g., bureau or office)	Bureau of Fiscal Services (BFS)	Bureau of Fiscal Services (BFS)	Bureau of Fiscal Services (BFS) Financial Management Service	CIO IT Administrators
Purpose of the Sharing	To manage CLM/iProcurement Application data pertaining to acquisitions, contracts, and procurement data transactions from/to BFS CIR.	To manage Public Sales Application data and credit card purchases through the CAS System.	To manage Office of Financial Management Application data to facilitate employee financial claim processing, payment, and identity verification.	To manage all MSS System Applications user access accounts, and to perform auditing and compliance activities.

PII Shared	<ul style="list-style-type: none"> • Vendor/Business Name • Point of Contact Name • Business Address • Ship to Location/Address • Business Phone Number • Business Email Address • Tax Identification Number (Tax ID) • CAGE Code (5-digit) - <i>Publically Available</i> • Dun & Bradstreet Business ID Number (D-U-N-S Number) (9-digit) <i>Publically Available</i> 	<ul style="list-style-type: none"> • Name of Purchaser/ Customer (e.g. Individual and/or Company) • Mailing Address • Telephone number • Email address • Order information: <ul style="list-style-type: none"> ○ Item ○ Price ○ Quantity ○ Order quote ○ Order number ○ Order date • Currency type (e.g. USD) • Customer/purchaser number • History of customer sales • Credit Card Information 	<ul style="list-style-type: none"> • Payee/Trading Partner/Supplier Name • Payee/Trading Partner/Supplier banking information • SSN/Tax ID number • Employee ID Number • Invoice number • Invoice date • Invoice approval status • Invoice amount • Purchase order number • Payment date • Payment Currency (e.g. USD) • Payment amount (partial, remaining, and/or total amount) • Payment Type (e.g. EFT, Check) • Supplier number 	<ul style="list-style-type: none"> • User Name/Login • Password • IP Address • Access Group Name • Metadata/User Access Statistical Information
Applicable Statutory or Regulatory Restrictions on Information Shared	N/A	N/A	N/A	N/A
Applicable Restrictions Imposed by Agreement on Information Shared (e.g., by Treasury agreement with the party that provided the information to Treasury)	N/A	N/A	N/A	N/A
Name and Description of MOU or Other Agreement Restricting Treasury's Internal Use, Maintenance, Handling, or Sharing of PII Received	N/A	N/A	N/A	
Method of PII Transfer (e.g., paper/oral disclosures/magnetic disk/portable device/email/fax/ot	<ul style="list-style-type: none"> • Electronic Interface 	<ul style="list-style-type: none"> • Electronic entry of Credit Card information into CC reader 	Secure electronic transmission	Network web portal

her (please describe if other)				
BEP limits its internal sharing of PII to BEP employees and contractors that have an official need to perform duties involving financial transactions or commercial purchases.				

Section 5.4: Information sharing with external (i.e., outside Treasury) organizations and individuals

External Information Sharing
<p>Section 5.4(a) <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No Is PII maintained in the system or by the project shared with agencies, organizations, or individuals external to Treasury?</p> <p>BEP shares PII from the Office of Financial Management Application with the GSA to reconcile travel claim reimbursement activities for BEP employees through the GSA Concur.Gov web portal/system.</p> <p>BEP shares information with the NFC to verify identities and EFT/banking information through BFS in order to facilitate non-payroll related payments to BEP employees.</p> <p>BEP may also share PII and statistical data from the Office of Financial Management and CLM/iProcurement Applications with GSA FPDS to permit the federal government to measure and assess the impact of procurements on the nation’s economy.</p> <p>BEP does not share PII from the Manufacturing Inventory and Manufacturing Execution Console Applications externally.</p>

Accounting of Disclosures
<p>Section 5.4(b) <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A With respect to <u>records</u> maintained in the system or by the project that are subject to the <u>Privacy Act</u>, do you maintain a paper or electronic log or other record of 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? <i>See 5 U.S.C § 552a(c).</i></p> <p>Section 5.4(c) <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A If you do not keep a running tabulation of every disclosure at the time it is made, are you able to reconstruct an accurate and complete accounting of disclosures so as to be able to respond to <u>Privacy Act</u> requests in a timely fashion?</p> <p>Section 5.4(d) <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A With respect to <u>records</u> maintained in the system or by the project that are subject to the <u>Privacy Act</u>, do you retain the log or other record of the date, nature, and purpose of each disclosure, for at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made?</p> <p>Section 5.4(e) <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> N/A With respect to <u>records</u> maintained in the system or by the project that are subject to the <u>Privacy Act</u>, does your bureau or office exempt the <u>system of records</u> (as allowed by the <u>Privacy Act</u> in certain circumstances) from the requirement to make the accounting available to the individual named in the record?</p> <p>Section 5.4(f) <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> N/A With respect to <u>records</u> maintained in the system or by the project that are subject to the <u>Privacy Act</u>, does your bureau or office exempt the <u>system of records</u> (as allowed by the <u>Privacy Act</u> in certain circumstances) from the requirement to inform any person or other agency about any correction or notation of dispute made by the agency of any <u>record</u> that has been disclosed to the person or agency if an accounting of the disclosure was made?</p> <p>These parameters apply to all applications under MSS.</p>

Statutory or Regulatory Restrictions on Disclosure
<p>Section 5.4(g) <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No In addition to the <u>Privacy Act</u>, are there any other statutory or regulatory restrictions on the sharing of any of the PII maintained in the system or by the project (e.g., 26 U.S.C § 6103 for tax returns and return information)?</p> <p>N/A. These parameters apply to all applications under MSS.</p>

Memorandum of Understanding Related to External Sharing

Section 5.4(h) Yes No N/A Has Treasury (including bureaus and offices) executed a Memorandum of Understanding, or entered into any other type of agreement, with any external agencies, organizations, or individuals with which/whom it shares PII maintained in the system or by the project?

N/A. These parameters apply to all applications under MSS.

Memorandum of Understanding Limiting Treasury's Use or Disclosure of PII

Section 5.4(i) Yes No Is any of the PII maintained in the system or by the project subject to the requirements of a Memorandum of Understanding or other agreement (e.g., agreement with another federal or state agency, an international agreement or treaty, or contract with private vendor that provided the information to Treasury or one of its bureaus) that limits or places conditions on Treasury's internal use or external (i.e., outside Treasury) sharing of the PII?

There are no agreements with entities outside of the Department of the Treasury. These parameters apply to all applications under MSS.

Memorandum of Understanding Limiting External Party's Use or Disclosure of PII

Section 5.4(j) Yes No Is any of the PII maintained in the system or by the project subject to the requirements of a Memorandum of Understanding or other agreement in which Treasury limits or places conditions on an external party's use, maintenance, handling, or disclosure of PII shared by Treasury?

N/A. These parameters apply to all applications under MSS.

External Information Sharing Chart

Section 5.4(k) Yes No Is information from the system or project shared externally?

External Recipient's Name	General Service Administration (GSA)	General Service Administration (GSA)	USDA NFC
System/Application	Office of Financial Management Application	CLM/iProcurement and Office of Financial Management Application	Office of Financial Management Application
Purpose of the Sharing	To reconcile travel claim reimbursement activities for BEP employees through the BFS FSM to GSA Concur.Gov.	To provide PII and statistical data to the FPDS to permit GSA to measure and assess the impact of federal procurement on the nation's economy.	To verify identities and EFT/banking information through the BFS FSM.
PII Shared	<ul style="list-style-type: none"> • Name • SSN • Date of Birth • Travel Dates • Travel Location • EFT/banking information • Home address • Business address • Business and personal telephone number • Travel Authorization number • Credit Card information • Reimbursable expenses 	<ul style="list-style-type: none"> • Vendor/Business Name • Point of Contact Name • Tax Identification Number (Tax ID) • CAGE Code (5-digit) - <i>Publically Available</i> • Dun & Bradstreet Business ID Number (D-U-N-S Number) (9-digit) <i>Publically Available</i> • Business Address • Ship to Location/Address 	<ul style="list-style-type: none"> • Name • SSN • EFT/banking information

	<ul style="list-style-type: none"> • Travel/lodging preferences • TSA Travel Redress number (if applicable) • TSA Known Traveler Number (if applicable) 	<ul style="list-style-type: none"> • Business Phone Number • Business Email Address • Invoice number • Invoice date • Invoice approval status • Invoice/purchase amount • Purchase order number • Supplier number • Date ordered • Order number • Order type • Statistical data 	
Content of Applicable Routine Use/Citation to the <u>SORN</u>	GSA/GOVT-4, Contracted Travel Services Program, Federal Register Volume 74, Number 105 (June 3, 2009)]	Treasury .009 – Treasury Fiscal Service Systems, Federal Register Volume 81, Number 215 (November 7, 2016)	GSA/GOVT-4, Contracted Travel Services Program, Federal Register Volume 74, Number 105 (June 3, 2009)]
Applicable Statutory or Regulatory or Restrictions on Information Shared	N/A	N/A	N/A
Name and Description of Relevant MOUs or Other Agreements Containing Sharing Restrictions Imposed on Treasury by an External Source or Source/Originating Agency (including description of restrictions imposed on use, maintenance, and disclosure of <u>PII</u>)	N/A	N/A	N/A
Name and Description of Relevant MOUs or Other Agreements Containing Restrictions Imposed by Treasury on External Sharing Partner (including description of restrictions imposed on use, maintenance, and disclosure of <u>PII</u>)	N/A	N/A	N/A
Method(s) Used to Transfer <u>PII</u> (e.g., paper/ oral disclosures/magnetic disk/portable device/email fax/other (please describe if other)	Electronically transmission through BFS to the GSA.	Electronically transmission to GSA.	Electronically transmission through BFS to the NFC.
All remaining information pertaining to the program and system remains within the Department of the Treasury.			

Obtaining Consent Prior to New Disclosures Not Included in the SORN or Authorized by the Privacy Act

Section 5.4(1) Yes No N/A Is the individual's consent obtained, where feasible and appropriate, prior to any **new** disclosures of previously collected records in a system of records (those not expressly authorized by the Privacy Act or contained in the published SORN (e.g., in the routine uses))?

These parameters apply to all applications under MSS.

Section 6: 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 6.1: Privacy Act System of Records Notice (SORN)

For collections of PII that meet certain requirements, the Privacy Act requires that the agency publish a SORN in the *Federal Register*.

System of Records

Section 6.1(a) Yes No Does the system or project retrieve records about an individual using an identifying number, symbol, or other identifying particular assigned to the individual? (see items selected in Section 4.2 above)

Section 6.1(b) Yes No N/A Was a SORN published in the *Federal Register* for this system of records?

Treasury/BEP .045 – Mail Order Sales Customer Files. This SORN will be amended to:

- 1) Add new categories of records:
 - telephone number,
 - email address,
 - order information (item, price, quantity, order number, order date, and order quote),
 - currency type,
 - customer number, and
 - inventory data

- 2) Discontinue using order number as a retrieval method and include additional retrieval methods:
 - mailing address,
 - telephone number,
 - email address, order information (item, price, quantity, order quote, order number, and order date),
 - currency type (e.g. USD),
 - history of customer sales, and
 - credit card information.

Treasury .009 – Treasury Fiscal Service Systems. BEP retrieves data from Treasury .009 by the Supplier/Business/Vendor name, Tax ID Number, or purchase order number related to the business or vendor.

Treasury .015 - General Information Technology Access Account Records. BEP retrieves data from Treasury .015 by Name, Computer Name or IP Address of the user.
GSA/GOVT-4 - Contracted Travel Services Program. BEP retrieves data from GSA/GOVT-4 by Name or Travel Authorization number, SSN or Employee ID Number (if available).

Section 6.2: 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 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).

Paperwork Reduction Act Compliance
<p>Section 6.2(a) <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No Does the system or project maintain information obtained from individuals and organizations who are not federal personnel or an agency of the federal government (i.e., outside the federal government)?</p>
<p>Section 6.2(b) <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A Does the project or system involve a new collection of <u>information in identifiable form</u> for 10 or more persons from outside the federal government?</p>
<p>Section 6.2(c) <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> N/A Did the project or system complete an Information Collection Request (“ICR”) and receive OMB approval?</p>
<p>6.2(a): The CLM/iProcurement Application, Office of Financial Management Application, Public Sales Application, and the Manufacturing Inventory Application maintain information from individuals or entities that are not federal personnel or part of the federal government. The Manufacturing Execution Console does not contain information on members of the public.</p>
<p>6.2(b): The CLM/iProcurement Application, Office of Financial Management Application, Public Sales Application, and the Manufacturing Inventory Application involve a collection of new information in an identifiable form for 10 or more persons outside of the federal government.</p>
<p>6.2(c): BEP receives information from BFS after individuals and business entities provide their PII and financial information to BFS Internet portals, which operate under the auspices of its own or Department of the Treasury information collection/public burden parameters.</p>
<p>The CLM/iProcurement Applications contain contract information and solicitation of proposals. This information collection receives coverage from the following OMB Control Numbers assigned to the Department of the Treasury: OMB Control Number 1505-0180 – Post-Contract Award Information and 1505-0181 – Solicitation of Proposal Information for Award of Contract.</p>
<p>There are no information requests or assigned OMB Control Numbers for the Public Sales, Financial Management, Manufacturing Inventory, or the Manufacturing Execution Console Applications.</p>

Section 6.3: 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 destroyed or sent to the NARA for permanent retention upon expiration of this period.

NARA Records Retention Requirements

Section 6.3(a) Yes No Are the records used in the system or by the project covered by NARA's General Records Schedules ("GRS") or Treasury/bureau Specific Records Schedule (SRS)? |

Section 6.3(b) Yes No N/A Did NARA approved a retention schedule for the records maintained in the system or by the project?

Section 6.3(c) Yes No N/A If NARA did not approve a retention schedule for the records maintained in the system or by the project and the records are not covered by NARA's GRS or Treasury/bureau SRS, has a draft retention schedule (approved by all applicable Treasury and/or Bureau officials) been developed for the records used in this project or system?

Office of Financial Management Application and CLM/iProcurement Applications:

- GRS 1.1: Financial Management and Reporting Records

Item 001 - DAA-GRS-2016-0013-0001 – Financial management and reporting administrative records. Temporary. Destroy when 3 years old, but longer retention is authorized if needed for business use.

Item 010 - DAA-GRS-2013-0003-0001 - Financial transaction records related to procuring goods and services, paying bills, collecting debts, and accounting. Temporary. Destroy 6 years after final payment or cancellation, but longer retention is authorized if required for business use.

Item 013 – DAA-GRS-2016-0001-0002 - Data submitted to the Federal Procurement Data System (FPDS). Temporary. Destroy or delete when 6 years old, but longer retention is authorized if required for business use.

Item 040 – DAA-GRS-2013-0003-0012 - Cost accounting for stores, inventory, and materials. Temporary. Destroy when 3 years old, but longer retention is authorized if required for business use.

Item 071 - DAA-GRS-2016-0001-0005 - Vendor and bidder information. Records of all other suspensions and debarments and all approved vendors and bidders. Temporary. Destroy 3 years after removal from approved status, but longer retention is authorized if required for business use.

Item 080 - DAA-GRS-2017-0005-0001 - Administrative claims by or against the United States. Temporary. Destroy 7 years after final action, but longer retention is authorized if required for business use.

- GRS 1.3: Budgeting Records

Item 010 – DAA-GRS-2015-0006-0001 - Budget Formulation, Estimates, Justification, and Submission Records, Fiscal Year 2017 and Forward. Temporary. Destroy 6 years after close of fiscal year, but longer retention is authorized if required for business use.

Item 020 - DAA-GRS-2015-0006-0002- Budget Execution Records. Temporary. Destroy 6 years after close of fiscal year, but longer retention is authorized if required for business use.

Item 030 – DAA-GRS-2015-0006-0003 – Budget Reports. Full fiscal-year reports. Temporary. Destroy when 5 years old, but longer retention is authorized if required for business use.

Item 030 – DAA-GRS-2015-0006-0004 – Budget Reports. All other reports. Temporary. Destroy when 3 years old, but longer retention is authorized if required for business use.

Item 040 – DAA-GRS-2015-0006-0006 – Budget Preparation Background Records. Records held in office responsible for preparing agency’s budget proposal to the White House. Temporary. Destroy 2 years after close of the fiscal year to which the records relate, but longer retention is authorized if required for business use.

Item 050 – DAA-GRS-2015-0006-0007 – Budget Administration Records. Temporary. Destroy when 3 years old, but longer retention is authorized if required for business use.

- BEP Records Control Schedule – 50.1 N1-318-04-10 – Financial Management

Item 1. CFO Annual Report. Records relating to the Chief Financial Officer's Annual Performance and Accountability Report for the Bureau. Official record copy. Permanent. Cut off files at end of each fiscal year and transfer to the BEP's records storage area 5 years after cutoff Transfer to NARA in five year blocks when the most recent record is 20 years old. Working files created in preparation of the CFO's Annual Report. Includes input reports from other offices. Temporary. Destroy 2 years after the close of the fiscal year covered by the annual Report.

Item 4. Credit Card Coordination Files. Files relating to coordination of Bureau credit cards issued to agency personnel for travel, procurement or other authorized use. Files include original credit card applications, monthly activity reports from credit card providers, and related correspondence and reports on credit card activity. Individual credit card applications. Temporary. Destroy when credit card is cancelled. All other records. Temporary. Destroy when 2 years old.

Item 5. Financial Management System Files, Records, and Reports. Electronic files, system reports, and hardcopy records documenting the collection, receipt, advance and reimbursement of funds; deposits, credits, debits, and disbursements of funds; and certification records documenting the authenticity of payment vouchers and other receipt and disbursement of funds. Financial documents and reports in hardcopy or electronic format that are required for BEP financial statement audit and financial accountability purposes. These records include periodic reports that are produced in the regular course of business, and special ad hoc or one-time only reports that are required for compliance with federal government financial accounting standards. Temporary. Destroy or delete 6 years and 3 months after the close of the fiscal year involved. Financial documents and reports in hardcopy or electronic format that are summarized or consolidated on a regular basis, and are not needed for financial statement audit or financial accountability purposes. Temporary. Destroy when superseded, updated, or obsolete, or when no longer needed for current agency business. All other records, reports, and electronic files that are created for one-time ad-hoc or special studies but which are not needed for financial statement audit or financial accountability purposes. Temporary. Destroy when no longer needed for current agency business.

- BEP Records Control Schedule – 50.2 N1-318-04-4 – Budget Formulation.

Item 1 – Final Budget Submissions. Official record copy of the consolidated Bureau budget estimate and justification submitted to Congress for review and approval. PERMANENT. Cut off files at the end of each fiscal year and transfer to the BEP's records storage area 5 years after cutoff. Offer to NARA in five year blocks when the most recent record is 20 years old.

Item 2 - Budget Correspondence and General Subject Files. Budget office correspondence, instructional materials, and other subject files documenting Bureau policies, procedures, and systems for developing and submitting internal budget data as prescribed by Department of Treasury and OMB requirements, and which reflect policy decisions affecting expenditures for Bureau programs. Temporary. Close inactive files and transfer to BEP's records storage area when 5 years old. Destroy when 7 years old.

Manufacturing Inventory Application and Manufacturing Execution Console Application:

- GRS 2.7: Employee Health and Safety Records

Item 040 - DAA-GRS-2017-0010-0004 - Workplace environmental monitoring and exposure records. Results or measurements of monitoring workplace air, toxic substances, or harmful physical agents,

including personal, area, grab, wipe, or other methods of sampling results. OSHA-regulated substance monitoring and exposure records. Temporary. Destroy no sooner than 30 years after monitoring is conducted, but longer retention is authorized if needed for business use. Occupational noise monitoring and exposure records. Temporary. Destroy no sooner than 2 years after monitoring is conducted, but longer retention is authorized if needed for business use.

- GRS 5.4: Facility, Equipment, Vehicle, Property, and Supply Records

Item 010 - DAA-GRS-2016-0011-0001 - Facility, Space, Vehicle, Equipment, Stock, And Supply Administrative And Operational Records. Temporary. Destroy when 3 years old or 3 years after superseded, as appropriate, but longer retention is authorized if required for business use.

Item 070 – DAA-GRS-2016-0011-0008 - Facility, Space, And Equipment Inspection, Maintenance, And Service Records. Temporary. Destroy when 3 years old, but longer retention is authorized if required for business use.

- BEP Records Control Schedule – 30.1 N1-318-04-25 – Management Control and Accountability.

Item 2 – ISO Quality Audits. Case files of internal quality audits of all quality activities relating to currency production and other Bureau functions as required by the ISO Quality Management Program. Files include final audit reports, correspondence, and records of meetings, checklists, verification of corrective actions, and supporting work papers and documentation. Official record copy contains final audit report and corrective action verification only. Temporary. Destroy 2 years after correction of cited deficiencies and/or reconciliation.

Item 3 – Audit Program Records. Records relating to planning, scheduling, and administration of the Bureau's internal audit program, including ISO quality audits. Files include annual audit plans, audit schedules, auditor rosters, auditor qualifications records, audit report logs, status reports, and related correspondence. Temporary. Destroy 8 years after completion of subsequent audit.

Item 7 - Outside Delivery Accountability - Records relating to accountability of security products delivered to an outside organization. Records include appropriate Requests for Assessment or authorizing memorandums, Print Orders, Orders for Supplies and Services, Transfer/ Delivery Schedules, verification of return or certificate of destruction, and other supporting documentation. Temporary. Destroy 2 years after return of item or receipt of proof of destruction.

- BEP Records Control Schedule – 70.1 N1-318-04-20 - Currency Production Records

Item 1 – Annual Currency Orders. Official Bureau records documenting the annual currency order from the Federal Reserve Board (FRB). Records include the FRB's written letters of request, the Bureau's order confirmation and detailed master delivery schedule, and other related correspondence and materials. Permanent. Cut off files at end of each fiscal year and transfer to the BEP's records storage area when volume warrants or when 5 years old. Transfer to NARA in five year blocks when the most recent record is 25 years old.

Item 2 - Currency Production History Records Production History Records (YCO Currency Process Sheet Record) documenting master schedule of serial numbers to be produced by denomination for each bank. Year-end final report: Permanent. Cut off files at end of each fiscal year and transfer to the BEP's records storage area when volume warrants or when 5 years old. Transfer to NARA in five year blocks when the most recent record is 25 years old. Interim monthly reports: Temporary. Destroy when superseded by next update.

Item 3. Currency Production Ordering and Scheduling. Official records of the production orders for currency-related printing and production activities, resource planning and production scheduling. Includes Print Orders, Orders for Supplies and Services, Manufacturing Orders, Work Authorizations. Temporary. Cut off files at end of each fiscal year. Destroy when 2 years old. Production scheduling records generated from the Yearly Currency Order system, including Monthly Delivery Schedules, Monthly Overprinting Requirements, Estimated Daily Production and Delivery Requirements,

Projected Press Schedule, Monthly Intaglio Plate Report. Temporary. Cut off files at end of each fiscal year. Destroy when 2 years old.

Item 6. Currency Manufacturing Support Materials. Production orders, schedules, reports, forms, logs and other records relating to support materials and equipment used in currency manufacturing, including roller manufacturing and recovery of inking-in and wiper rollers. Temporary. Destroy after 1 year.

Item 7. Currency Production Analytical Reports. Routine management reports to monitor and analyze productivity, spoilage, and inventory accuracy, returns, and other production data. Reports are compiled and distributed by Production Management. Temporary. Cut off files at end of each fiscal year. Destroy when 2 years old.

- BEP Records Control Schedule – 70.2. N1-318-09-01

Item 1. Operational Records. Product Accountability and Load Forms. Temporary. Cut off files at end of each fiscal year. Destroy when 2 years old. Other Operations Data and Control Forms. Temporary. Cut off files at end of each fiscal year. Destroy when most recent file is 1 year old. Daily Production Summary Reports Summary reports of daily currency printing and processing statistics, equipment downtime, shift staffing, and other routine operational activities. Files are maintained with associated currency production sections. Temporary. Cut off files at end of each fiscal year. Destroy when most recent file is 1 year old.

- BEP Records Control Schedule – 70.4. N1-318-04-19.

Item 1. Engraving and Plate Production. Files containing documentation of production and control of engraving plates, dies, rolls, seals, and other miscellaneous items used in the production of U. S. government securities and postage stamps produced by the Bureau. Temporary. Retain in active engraving files until plate is cancelled. Transfer cancelled plate files to BEP's records storage area. Destroy 30 years after cancellation of plate or request NARA's permission to transfer to an interested numismatic/philatelic organization. Tracking logs, maintained electronically, include Engraving Offset Plate Number Assignment, Engraving Items of Reproduction Number Assignment, and Engineering Rework Surface Piece Assignment logs. Files previously maintained on typed index cards. Temporary. Update as needed for current business and delete electronic version when no longer needed for administrative, legal, audit, or other operational purposes.

- BEP Records Control Schedule – 70.6. N1-318-04-14.

Item 1. Materials Requirements Files. Files on annual usage forecast for currency paper, currency inks, and other production materials, delivery schedules, and monthly inventory tracking, based on Yearly Currency Order and revisions. Information is maintained in electronic spreadsheet system, Materials Requirements Plan (MRP) System. Temporary. Destroy when 2 years old. Interim reports. Temporary. Destroy when superseded.

Item 2. Supplier Files (COTR Files). Working files maintained by program analysts containing contract documents and modifications, statements of work, product specifications, correspondence, reports, and other information relating to monitoring and analysis of supplier deliveries, inventory balances, product conformance, etc. Temporary. Destroy 2 years after contract is completed.

Item 3. Storeroom and Warehouse Inventory Requisition and Distribution Files. Files include requisition forms, order summaries, checklists, logs, control sheets, and other documentation of storeroom and warehouse inventory and distribution management. Contain various official Bureau forms and other intimal logs and control sheets. Temporary. Destroy 2 years after currency is issued and 2 years after ink supply is entered into production.

Item 4. Cyclic Inventory Control Report Files. Work package files for daily cycle count inventories conducted to verify physical inventory of items against BEPMIS inventory. Temporary. Destroy 1 year after reconciliation of inventory.

Item 5. Currency Materials Inspection and Testing. Records documenting the inspection and testing of currency materials, and verifications and certifications that the materials conform to applicable production specifications and contract requirements. Materials required to undergo testing include currency papers, currency inks and rollers, and miscellaneous materials that are acquired under contract or by the simplified acquisition process, and currency inks manufactured by the Bureau. Test Records. Temporary. Destroy when 2 years old. Non-conforming Materials Reports. Temporary. Destroy 2 years after correction of nonconformance.

- BEP Records Control Schedule – 7.7. N1-318-04-13. Ink Design and Manufacturing

Item 1. Ink Research and Design. Records relating to the research and development of new currency inks used for printing U.S. currency and other security products. Permanent. Cut off subject files when 5 years old or when associated project is complete. Retire to BEP's records storage area when volume warrants. Transfer to NARA 25 years after cutoff.

Item 2. Ink Manufacturing. Production orders, schedules, reports, forms, logs, and other records that identify and control currency ink manufacturing activities, accountability and traceability of materials, daily production statistics, and other production information. Orders to Manufacture, Report of Production Batch Samples, Batch Summary Reports. Temporary. Cut off files at end of each fiscal year. Destroy when 2 years old. All other records. Temporary. Destroy after 1 year or when no longer needed.

- BEP Records Control Schedule – 100.1 N1-318-04-24 - Environment, Safety and Occupational Health Records

Item 3. Clean Air Emissions Records. Records relating to permitting and managing the Bureau's operations and equipment to prevent or minimize the amount of air pollutants emitted from Bureau operations to the outside air to ensure compliance with the Clean Air Act, and associated state and local regulations. Records include permit applications and supporting documentation, permits, approvals for new construction or modifications to equipment or changes in raw materials, monitoring plans and procedures, volatile organic compound limits (VOC) for inks, wiping, and dampening solutions, and other products used in Bureau operations, equipment documentation, monitoring data and analysis, and other documentation required by the permit. Temporary. Destroy 3 years after related permit expires. Annual Air Report. Temporary. Destroy 15 years after related permit expires. Notification and Compliance Testing for Hard Chromium Plating Operations. Temporary. Maintain until equipment is removed, then destroy.

Item 6. Occupational Health and Safety Program Files. Annual Health and Safety Reports, Employee Safety Suggestion Reviews, Safety Document reviews. Temporary. Destroy when 5 years old. Confined space inventory, control of hazardous energy inventory and procedures. Temporary. Destroy when superseded, obsolete, or no longer in use.

Public Sales Application:

- BEP Records Control Schedule – 10.2 N1-318-04-21 - Public Services.

Item 2 – Public Sales: Hardcopy and electronic records relating to sale of currency products and souvenirs to the public, via the public Web Site or Visitor Center. Includes records on products available for sale, customer orders and payment transactions, inventory status and restocking, summary reports of sales, related correspondence and supporting materials. Hardcopy records. Temporary. Destroy after audit or when 3 years old, whichever is later. Electronic Records. Temporary. Destroy after 3 years old or when no longer needed for administrative, legal, fiscal, audit, or other operational purpose (if hardcopy is record).

MSS System and Applications:

- BEP Records Control Schedule – 80.1 N1-318-04-2. Information Systems

Item 1. Bureau of Engraving and Printing Management Information System (BEPMIS) - Hardcopy and electronic records of the Bureau's primary integrated financial, manufacturing, and product accountability system. BEPMIS is composed of many different modules and applications which support product accountability, inventory control, work-in-progress, accounting, and other Bureau activities. Many of the records created and maintained within BEPMIS are scheduled separately with related records for the appropriate functional activities. Electronic data. Permanent. Transfer to NARA when 30 years old. All other files. Temporary. Close out files at end of each fiscal year. Hold in office at least 7 years, then delete when no longer needed.

SORN Record Schedules:

- Treasury .009, Treasury Fiscal Service Systems Records maintenance and disposal is in accordance with National Archives and Records Administration retention schedules, and any supplemental guidance issued by individual components.
- Treasury .015, General Information Technology Access and Accounts Records are maintained in accordance with the National Archives and Records Administration's General Records Schedule 24, section 6, "User Identification, Profiles, Authorizations, and Password Files." Inactive records will be destroyed or deleted 6 years after the user account is terminated or password is altered, or when no longer needed for investigative or security purposes, whichever is later.
- GSA/GOVT-4 – Contracted Travel Services Program Records kept by a Federal agency are maintained in accordance with the General Records Retention Schedules issued by the National Archives and Records Administration (NARA) or an agency and NARA approved records disposition schedule.
- Treasury/BEP .045 - Mail Order Sales Customer Files are retained and disposed in accordance with BEP Records Retention and Disposal Schedule No. 21 (N1/318/04/21) approved by the National Archives and Records Administration (NARA).

Section 6.4: 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"). Different security requirements apply to National Security Systems.

Federal Information System Subject to FISMA Security Assessment and Authorization

Section 6.4(a) Yes No N/A Is the system a federal information system subject to FISMA requirements?

Section 6.4(b) Yes No N/A Has the system or project undergone a SA&A and received ATO?

MSS received its Security Assessment and ATO on October 27, 2018, based on an initial assessment and Privacy Threshold Analysis (PTA) that deemed the system non-privacy sensitive. An additional comprehensive review discovered new PII collection of members of the public, and changes in the interfaces and functionality, which triggered this PCLIA.

Access Controls and Security Requirements

Section 6.4(c) Yes No Does the system or project include access controls to ensure limited access to information maintained by the system or project?

BEP assigns personnel to specific groups within its Active Directory, which serves as a tool for granting role-based access. In addition, BEP uses its Identity and Access Management System (IDM) to process access requests and conduct identity verification and authentication. Groups within the Active Director range from normal users to system administrators. System administrators provide additional access controls within MSS by

assigning authorized users to a particular application or applications based on the individual's need to access the information in the performance of their official duties. BEP limits access to the MSS to the Office of Acquisitions, the Office of Financial Management, the Office of Engraving (DCF/WCF), the Office of Currency Manufacturing (DCF/WCF), the Office of Compliance (DCF/WCF), the Office of Quality Operations (DCF/WCF), the Office of Quality Engineering and Management (WCF), the Office of Facilities Support (DCF), the Facilities Management Division (WCF), the Office of Security (DCF), the Security Division (WCF) and the Office of Environment, Health, and Safety (DCF/WCF), the Office of External Relations, and the CIO. These individuals operate the system in the performance of their official duties.

Security Risks in Manner of Collection

Section 6.4(d) Yes No In **Section 4.3** above, you identified the sources for information used in the system or project and the method and manner of collection. Were any security, privacy, or civil liberties risks identified with respect to the manner in which the information is collected from the source(s)?

BEP reduces its security and privacy risks by collecting information directly from individuals or business entities when practical and/or receiving the information from federal financial services Internet portals after entry by the individual.

BEP collects information used by the CLM/iProcurement and the Office of Financial Management Applications from BFS after it is entered by the individual or business entity into the CIR System. Security and privacy risks are reduced substantially by individuals/entities submitting their information directly to BFS. BEP may update information obtained directly from the individual or entity.

BEP reduces security and privacy risks of data collected for the Public Sales application by no longer operating a public-facing commercial numismatic purchases website. This mitigates the risk of collecting incorrect information. Individuals or entities may conduct orders through the U.S. Mint or by postal mail or telephone. The postal mail and telephone transactions require follow-up calls to retrieve credit card numbers that are not stored in MSS. Purchasers are not granted access to the Public Sales or Manufacturing Inventory Applications, where data is entered by OEX personnel. Therefore, minimal data collection from the public reduces security, privacy, or civil liberties risks.

BEP does not collect information from the public for use in the Manufacturing Execution Console.

Security and Privacy risks for the MSS System are mitigated by limiting access to BEP personnel with a need to access the system for official purposes.

Security Controls When Sharing Internally or Externally

Section 6.4(e) Yes No N/A Are all Treasury/bureau security requirements met in the method of transferring information (e.g., bulk transfer, direct access by recipient, portable disk, paper) from the Treasury project or system to internal or external parties?

The system meets federal information security requirements and operates under an existing Security Authorization and ATO. BEP will only share the PII of individuals or business entities in a secure manner that meets all federal standards.

Monitoring of Individuals

Section 6.4(f) Yes No Will this system or project have the capability to identify, locate, and monitor individuals or groups of people?

N/A. These parameters apply to all applications under MSS.

Audit Trails

Section 6.4(g) Yes No Are audit trails regularly reviewed for appropriate use, handling, and disclosure of PII maintained in the system or by the project inside or outside of the Department?

The BEP CIO Directorate conducts periodical audits of all IT systems in order to monitor user activity and to ensure that data is not exposed to unauthorized individuals. MSS Administrators also create and manage all accounts and conduct technical modifications.

Section 6.5: 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.

Applicability of and Compliance With the Rehabilitation Act

Section 6.5(a) Yes No Will the project or system 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)?

Section 6.5(b) Yes No N/A Does the system or project comply with and/or employ various 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?

BEP MSS is not accessible by members of the public and is restricted to the BEP workforce designated in Section 6.4c above. BEP performs a continuous review in order to (1) determine the user community, (2) employ various accessibility features into its software products, and (3) to procure specific tools for personnel use in compliance with Section 508 of the Rehabilitation Act, as amended in 1998. Should a disabled employee require access to information from the system, BEP will provide the information to the employee in an appropriate and preferred format for the individual.

Members of the public that access BFS’ website and systems to provide financial information for use in the CLM/iProcurement and Office of Financial Management Applications are assured that BFS is committed to making its website accessible to everyone. To meet this commitment, they strive to make the site compliant with the requirements of Section 508. The website is designed to be equally accessible to those using current, standards-compliant web browsers or assistive technologies. Achieving compliance with Section 508 is an ongoing process. If individuals or business entities have difficulty accessing any of their web pages or have questions about accessing information on a particular page, they may e-mail BFS.

Section 7: Redress

Access Under the Freedom of Information Act and Privacy Act

Section 7.0(a) Yes No Does the agency have a published process in place by which individuals may seek records under the Freedom of Information Act and Privacy Act?

The Treasury/bureaus FOIA and PA disclosure regulations can be found at 31 C.F.R. Part 1, Subtitle A, Subparts A and C.

Privacy Act Access Exemption

Section 7.0(b) Yes No Was any of the information that is maintained in system of records and used in the system or project exempted from the access provisions of the Privacy Act?

These parameters apply to all applicable SORNS associated with MSS.

Additional Redress Mechanisms

Section 7.0(c) Yes No With respect to information maintained by the project or system (whether or not it is covered by the Privacy Act), does the bureau or office that owns the project or system have any additional mechanisms other than Privacy Act and FOIA remedies (e.g., a customer satisfaction unit; a complaint process) by which an individual may request access to and/or amendment of their information and/or contest adverse determinations about denial of their rights, benefits, and privileges under federal programs (e.g., decisions about whether the individual will receive a financial benefit, get a clearance or access to a Treasury facility, obtain employment with Treasury)?

Business entities, suppliers, and vendors submit their own information to federal financial services Internet portals or when providing information to facilitate commercial/public numismatic product purchases. BEP

permits customers to correct their information (including financial data) at the time of initial or subsequent submission in addition to pursuing redress through the Privacy Act and FOIA processes. BEP employees may change or correct their information at their discretion within BEP, Treasury, or federal human resources and financial databases.

Responsible Officials

Bureau Privacy Official
Anthony Johnson
Government Information Specialist (Privacy)
Office of Critical Infrastructure and IT Security
Bureau of Engraving and Printing
Department of the Treasury

Reviewing Official
Michael J. Pease
Chief, Office of Critical Infrastructure and IT Security
Bureau of Engraving and Printing
Department of the Treasury

Approval Signature

//S// (mm/dd/yy)

Michael J. Pease
Chief, Office of Critical Infrastructure and IT Security

ATTACHMENT I

Public Sales Application: OEX performed a PCLIA to determine whether the routine uses are compatible with the original purpose for which the records were collected. These records may be used to disclose information:

- (1) To financial institutions processing credit card payments for numismatic and engraved purchases.

Compatibility: In order to complete numismatic and engraved products purchases either through its Gift Shop or from bulk purchases, BEP must collect credit card information and share it with financial institutions processing the payment. This disclosure is compatible and consistent with the original purpose of collection because it allows BEP to complete the purchase.

- (2) To consumer reporting agencies concerning a U.S. Government claim against an individual in accordance with 5 U.S.C. 552a(b)(12) and Section 3 of the Debt Collection Act of 1982 (Pub. L. 97-365), to encourage repayment of an overdue debt.

Compatibility: This disclosure is compatible with the original collection as it relates to BEP's requirement to report debts owed to the Federal government by numismatic product purchasers. BEP may have to retrieve information from record sources and provide the information to debt collection services.

- (3) To appropriate agencies, entities, and persons when (1) the Department and/or BEP suspects or has confirmed that there has been a breach of the system of records; (2) the Department and/or BEP has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the Department and/or BEP (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department and/or BEP efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

Compatibility: Individuals making numismatic and engraved product purchases must submit personally identifiable information to BEP in order to facilitate sale and delivery of these products. OMB Memorandum 17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information," dated January 3, 2017, requires adding a routine use to disclose information to appropriate agencies, entities, and persons to assist BEP in responding to a breach jeopardizing the integrity, confidentiality, or availability of the information maintained about individuals in the system of records.