



Privacy and Civil Liberties Impact Assessment Update  
for the

**Drug-Free Federal Workplace System**

January 23, 2018

**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**

BEP is required to use the Federal Drug Testing Custody and Control Form (CCF), as developed by the Department of Health and Human Services (HHS), Substance Abuse and Mental Health Services Administration and approved by the Office of Management and Budget (OMB) for urine drug testing. Historically, the CCF has been available for use in paper form. On May 28, 2014, OMB approved the use of both a paper form CCF and an electronic CCF (eCCF) under the HHS Mandatory Guidelines for Federal Workplace Drug Testing Programs. This PCLIA update addresses BEP's efforts to automate the CCF and make the eCCF available in BEP's Drug-Free Federal Workplace Program System. The eCCF requires the same collection of information and distribution of information to the relevant parties (i.e. test facility, employer, donor, collector, Medical Review Officer (MRO)) as the paper CCF but via a secure Internet-based application.

## **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 Drug-Free Federal Workplace Program (DFFWP) was established by Executive Order (EO) 12564<sup>1</sup> on September 15, 1986, to address illegal drug use by federal employees. The Office of Security in Washington, D.C. (DCF) and the Security Division in Fort Worth, TX (WCF) are responsible for implementing, coordinating, and managing the DFFWP in the Bureau of Engraving and Printing (BEP). The BEP uses the DFFW System (DFFWS) to track and maintain records such as drug screening activities, operations, and associated reports pertaining to BEP employees and applicants.

The DFFWS provides program managers the capability to select employees for random drug screening. BEP will continue to use a manual employee roster obtained from its human resource management system, arranged by employee name and employee identification number, to provide

---

<sup>1</sup> [E.O. 12564](#).

the initial random screening pool of individuals. The DFFWS will interface with the BEP email system in order to deliver notification letters to the managers and supervisors of employees selected randomly for drug screening. The DFFWS will also interface with the BEP personnel security system to obtain the security clearance level of employees assigned to positions involving national security or are sensitive in nature in order to add these individuals to the random selection pool. The DFFWS interface boundary will not involve connectivity to external relevant parties i.e. collector, test facility, or the Medical Review Officer (MRO). BEP will manually share personnel rosters or reports from the DFFWS on individuals scheduled for screening with external relevant parties and BEP program managers and supervisors as needed. BEP will also use the DFFWS to store individual testing results.

BEP currently uses the paper form of the Federal Drug Testing Custody and Control Form (CCF), as developed by the Department of Health and Human Services (HHS), Substance Abuse and Mental Health Services Administration and approved by the Office of Management and Budget (OMB) for urine drug testing. DFFWP does not maintain the CCF. The update to DFFWS includes an electronic CCF (eCCF) module that automates the CCF used for drug test ordering, specimen collection processing, and chain of custody documentation. With the approved eCCF, HHS is not requiring collection of any new or different information. The only change from the paper CCF to the eCCF is the mechanism for collecting and transmitting the requisite information. The eCCF documents the external specimen chain of custody — i.e., drug test specimen handling from the time it is collected until it is received at the laboratory. The eCCF also documents the final laboratory results reported to the MRO — the BEP Trusted Agent and licensed physician responsible for managing and verifying screening results. The eCCF requires the same collection of information and distribution of information to the relevant parties (i.e. test facility, employer, donor, collector, Medical Review Officer (MRO)) as the paper CCF but via a secure Internet-based application.

The eCCF increases data accuracy, eliminates form legibility issues, expedites drug screening collections, streamlines delivery of eCCF copies to appropriate stakeholders, reduces paperwork, and increases overall efficiency and program credibility.

Additionally, the system will store information pertaining to the specimen, laboratory, collection location, and PII on individuals involved in the chain of custody. This electronic system enhances security, sample handling, and the overall credibility of the program.

**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,<sup>2</sup> 5 U.S.C. § 3301(2),<sup>3</sup> 5 U.S.C. § 7301,<sup>4</sup> 31 U.S.C. § 303,<sup>5</sup> 31 U.S.C. 5141, Section 503 of Pub. L. 100-71, Mandatory Guidelines for Federal Workplace Drug Screening Programs,<sup>6</sup> and Executive Order No. 12564, Drug-Free Federal Workplace.<sup>7</sup>

## 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 an existing paper CCF promulgated by the Department of Health and Human Services and approved by OMB. The eCCF operates under the auspices of an OMB Control Number assigned to the Federal drug screening program. Additionally, BEP used the Privacy Threshold Analysis (PTA) process to assess the PII to ensure that it only collects the minimal amount necessarily to allow BEP to manage the DFFWP. BEP is

<sup>2</sup> 5 U.S.C. § 301.

<sup>3</sup> 5 U.S.C. § 3301(2).

<sup>4</sup> 5 U.S.C. § 7301.

<sup>5</sup> 31 U.S.C. § 303.

<sup>6</sup> Section 503 of Pub. L. 100-71.

<sup>7</sup> E.O. 12564.

pursuing administrative changes to reduce SSN collection by using an employee's Human Resource Account Number (HRConnect Number) in lieu of the SSN for matching samples and results to the correct individual. BEP incorporated a new 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. Although SSN collection from individuals remains voluntary, the DFFWP Administrator maintains access to the individual's SSN for identity verification and sample matching purposes to distinguish between individuals that may have the same name or other matching PII.

## **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.

<b>Biographical/General Information</b>		
<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 checked="" 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 checked="" 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 checked="" type="checkbox"/> Other (please describe): Tested Individual's Job Title
<input type="checkbox"/> Other (please describe):	<input type="checkbox"/> Other (please describe):	<input type="checkbox"/> Other (please describe):

### **Identifying Numbers**

Full Social Security number (voluntarily provided)     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 type="checkbox"/> Business Taxpayer Identification Number (If known: <input type="checkbox"/> sole proprietor; <input type="checkbox"/> non-sole proprietor)
<input type="checkbox"/> Personal Credit Card Number	<input 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 type="checkbox"/> Business Bank Account Number	<input 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 type="checkbox"/> Other Identifying Numbers (please describe):
<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): Specimen ID 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 checked="" type="checkbox"/> Other (please describe): Drug test type and test results (positive or negative).		

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	<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 checked="" type="checkbox"/> Other (please describe): Drug Test Samples	<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 checked="" 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 type="checkbox"/> Other (please describe): _____

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 statistical data.	<input type="checkbox"/> Other (please describe):	<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): _____

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

Drug Test Subject	Contractor/Collector	Laboratory/MRO	DFFWP Administrators (Users)
<p><b>Specific PII identified in Section 4.2 acquired from this source:</b></p> <ul style="list-style-type: none"> <li>Name</li> <li>Social Security Number (SSN) (voluntarily provided)</li> <li>Date of Birth</li> <li>Business/Home Address</li> <li>Business/Home Phone Number</li> <li>Job Title</li> <li>Email Address</li> <li>Office Name</li> <li>Security Clearance Level</li> <li>Drug Sample Number</li> <li>Test results</li> </ul>	<p><b>Specific PII identified in Section 4.2 acquired from this source:</b></p> <ul style="list-style-type: none"> <li>Name</li> <li>Business Name</li> <li>Business Address</li> <li>Business/Mobile Phone Number</li> <li>Email Address</li> </ul> <p>Collected by the Office of Physical Security for individuals requiring access to BEP facilities. This data is covered by existing privacy compliance documentation.</p> <ul style="list-style-type: none"> <li>Photograph</li> </ul>	<p><b>Specific PII identified in Section 4.2 acquired from this source:</b></p> <ul style="list-style-type: none"> <li>Name</li> <li>Business Name</li> <li>Business Address</li> <li>Business/Mobile Phone Number</li> <li>Email Address</li> </ul>	<p><b>Specific PII identified in Section 4.2 acquired from this source:</b></p> <ul style="list-style-type: none"> <li>User Name/Login</li> <li>Password</li> <li>IP Address</li> <li>Access Group Name</li> <li>Metadata/User Access Statistical Information</li> </ul>

	<ul style="list-style-type: none"> <li>• Name</li> <li>• Business Name</li> <li>• Supervisory status</li> <li>• Section (specific area in the building)</li> <li>• Date access badge issued</li> <li>• Security Control Point Date, Time, and Location.</li> </ul>		
<b>Manner in which information is acquired from source by the Treasury project/system: (select all that apply):</b>	<b>Manner in which information is acquired from source by the Treasury project/system: (select all that apply):</b>	<b>Manner in which information is acquired from source by the Treasury project/system: (select all that apply):</b>	<b>Manner in which information is acquired from source by the Treasury project/system: (select all that apply):</b>
<input checked="" type="checkbox"/> From a paper or electronic form provided to individuals, the public or members of a particular group	<input type="checkbox"/> From a paper or electronic form provided to individuals, the public or members of a particular group	<input type="checkbox"/> From a paper or electronic form provided to individuals, the public or members of a particular group	<input type="checkbox"/> From a paper or electronic form provided to individuals, the public or members of a particular group
Please identify the form name (or description) and/or number (e.g., OMB Control Number): Unnumbered Custody Control Form (CCF) and/or eCCF. OMB Control No. 0930-0158 (Donor's initials only)	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): _____	Please identify the form name (or description) and/or number (e.g., OMB Control Number): _____
<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"/> 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 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 type="checkbox"/> Email	<input checked="" type="checkbox"/> Email	<input checked="" 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 checked="" type="checkbox"/> Extracted from particular technology (e.g., radio frequency identification data (RFID) devices, video or photographic cameras, biometric collection devices): Badge Photo	<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 checked="" type="checkbox"/> Fax	<input checked="" 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: PII extracted from existing Human Resource (HR) Databases.	<input type="checkbox"/> Other: Please describe: _____	<input type="checkbox"/> Other: Please describe: _____	<input checked="" type="checkbox"/> Other: Please describe: Extracted from system access and audit logs.
<input checked="" type="checkbox"/> Other: Please describe: Drug sample collected directly from individual.	<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©(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.
- The effects on the individual, if any, if they decide not to provide all or any part of the requested information.

##### **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).

**Section 4.4(d)**  Yes  No  N/A Does the system or project maintain SSNs?

**Section 4.4(e)**  Yes  No  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.

**Section 4.4(f)**  Yes  No  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::

- SSN disclosure is required by Federal statute or Executive Order. ; or
- the SSN is disclosed to any Federal, state, or local agency maintaining a system of records 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. *If checked, please provide the name of the system of records in the space provided below:*

**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.

BEP provides notice that collection of the SSN is voluntary on the collection form. BEP subsequently eliminated SSN collection by using an employee’s Human Resource Employee ID Number in lieu of the SSN for matching samples and results to the correct individual. Although SSN collection from individuals remains voluntary, the DFFWP Administrator maintains access to the individual’s SSN for identity verification and sample matching purposes to distinguish between individuals that may have the same name or other matching PII. The authorities for this collection, which is associated with the Department of Health and Human Services (HHS), the federal entity that manages the overall program are 5 U.S.C. § 301, 5 U.S.C. § 3301(2), 5 U.S.C. § 7301, 31 U.S.C. § 303, 31 U.S.C. 5141, Section 503 of Pub. L. 100-71, Mandatory Guidelines for Federal Workplace Drug Screening Programs, and Executive Order No. 12564, Drug-Free Federal Workplace. Executive Order 12584.

### 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

## **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.

In order to operate its currency and security documents manufacturing operations, BEP must ensure a safe and healthy work environment. As noted in Section 4.2, BEP uses biographical PII to ensure that the testing sample matches the correct individual and to contact employees, employment applicants, contractors responsible for collecting and handling testing samples, test facility/laboratory personnel, and MROs in order to communicate with these entities when appropriate in order to address matters pertaining to collections, drug samples, and testing results. The information is also used to grant access to BEP facilities to contractors that collect/handle samples. Identifying numbers, including employee ID numbers and Social Security numbers, are collected from employees and employment applicants to ensure that the sample matches the correct individual throughout each phase of the DFFWP Program. BEP collects medical information (e.g. test types and testing results) on employees and employment applicants from test facility/laboratory personnel, which is used to determine employment eligibility. Audit log and security monitoring information, including statistical metadata, is collected from DFFWPS administrators (system users).

BEP collects and stores system data, including user login/password information, meta-data, and statistical data to manage accounts and access to the system.

### **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?

BEP collects names and PII from existing HR systems in order to build the random selection database. Drug testing samples are collected directly from the individual. The eCCF is pre-populated with PII pertaining to the individual. BEP obtains the individual's initial on form.

The remaining information consists of contact information and is collected directly from the contractor/collector, laboratory personnel, or the MRO when appropriate.

## 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?

No privacy and civil liberties risks were identified.

## 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?

## 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.

### 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? *to make determinations about an individual you selected “no” because you do not use information in the system or project to make determinations about individuals*

BEP ensures the accuracy, relevance, completeness, and timeliness of the information it maintains or transmits in the system by collecting the information directly from the individual strategic partner or vendor. In certain instances, the information is collected from corporate representatives that receive the information directly from onboarding contractors. Since the corporate representative collects the PII directly from the individual to whom it pertains, the risk of collecting inaccurate information is minimized.



## 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?

There are no automated mechanisms for merging PII obtained from HR systems into the DFFWS. The DFFWP Administrator will use the system to pre-populate data fields in the eCCF that the individual will present to the collection official.

Since the DFFWP Administrator collects the PII directly from established HR systems and presents the information on the eCCF to the individual for verification purposes, risk of collecting inaccurate, irrelevant, untimely, or incomplete information is minimized.

Information collected from the Contractor/Collector originates from the Administrative Security program and associated systems is also collected directly from the individuals and is deemed accurate, relevant, timely, and complete.

Contact information collected directly from the Contractor pertaining to Laboratory personnel or the MRO is also deemed accurate, relevant, timely, and complete.

## 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)?

Individuals subject to drug testing have the opportunity to review the eCCF for accuracy prior to testing. The eCCF reduces the likelihood of inaccurate information by allowing the DFFWP Administrator to make corrections directly in the database if there are discrepancies.

## 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 the DFFWP Administrator collects the PII directly from the established HR system or the individual to whom it pertains, BEP deems this information accurate. The Contractor/Collector provides information pertaining to Laboratory Personnel and the MRO directly to BEP.

### 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 DFFWS is not the primary source of PII obtained by the DFFWP Administrator to populate random pools. Once PII is obtained from HR resources and combined with the automated information within the eCCF, it then serves as the Privacy Act System of Records and may be used to transmit information subject to the Privacy Act. This activity includes provisions requiring the dissemination of information pertaining to correction or amendment of PII and notification of impacted individuals. Contractor/Collectors, Laboratory Personnel, or the MRO may correct their contact information at any time. Users may also access and update their information at any time.

## Section 5.3: Information sharing within the Department of the Treasury

### Internal Information Sharing

**Section 5.3(a)**  Yes  No 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")?

### 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

### Internal Information Sharing Chart

Internal Recipient's Name (e.g., bureau or office)	BEP DFFWP Administrators (Users) within the Office of Security (Washington, DC Facility) and the Security Division (Forth Worth, TX Facility)	CIO IT Administrators	Supervisors/Managers

Purpose of the Sharing	To manage the program and develop the drug testing pools of individuals.  To address specific instances of positive test results.	To manage user access accounts, and to perform auditing and compliance activities.	To notify employees that they have been selected for drug testing.
PII Shared	<ul style="list-style-type: none"> <li>• Name</li> <li>• Date of Birth</li> <li>• Social Security Number (SSN)</li> <li>• Employee ID Number</li> <li>• Business/Home Address</li> <li>• Business/Home Phone Number</li> <li>• Email Address</li> <li>• Job Title</li> <li>• Office</li> <li>• Drug test type</li> <li>• Test results</li> </ul>	<ul style="list-style-type: none"> <li>• User Name/Login</li> <li>• Password</li> <li>• IP Address</li> <li>• Access Group Name</li> <li>• Metadata/User Access Statistical Information</li> </ul>	<ul style="list-style-type: none"> <li>• Name</li> <li>• Date, time, location of testing</li> <li>• Results/information pertaining to positive tests.</li> <li>• Drug test type</li> </ul>
Applicable Statutory or Regulatory Restrictions on Information Shared	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
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/other (please describe if other))	Paper, Email (including attached documents), Network Web Portal (including free text fields), and regular mail between facilities when needed.	Network web portal.	Email
BEP limits sharing information from the DFFWS with internal offices and personnel that have an official need to inform their personnel that they have been selected for drug testing. BEP also limits sharing reports and statistical data to managers and leadership that have a need to know the information. BEP also limits sharing to system managers responsible for maintain the system and managing user accounts and access.			

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

**External Information Sharing**

**Section 5.4(a)**  Yes  No Is PII maintained in the system or by the project shared with agencies, organizations, or individuals external to Treasury?

N/A. Information shared with contracted personnel i.e., collections/test facility.

**Accounting of Disclosures**

**Section 5.4(b)**  Yes  No  N/A With respect to records maintained in the system or by the project that are subject to the Privacy Act, 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? See 5 U.S.C § 552a(c).

**Section 5.4(c)**  Yes  No  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 Privacy Act requests in a timely fashion?

**Section 5.4(d)**  Yes  No  N/A With respect to records maintained in the system or by the project that are subject to the Privacy Act, 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?

**Section 5.4(e)**  Yes  No  N/A With respect to records maintained in the system or by the project that are subject to the Privacy Act, does your bureau or office exempt the system of records (as allowed by the Privacy Act in certain circumstances) from the requirement to make the accounting available to the individual named in the record?

**Section 5.4(f)**  Yes  No  N/A With respect to records maintained in the system or by the project that are subject to the Privacy Act, does your bureau or office exempt the system of records (as allowed by the Privacy Act 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 record that has been disclosed to the person or agency if an accounting of the disclosure was made?

Recruiting, Examining, and Placement Records

**Statutory or Regulatory Restrictions on Disclosure**

**Section 5.4(g)**  Yes  No In addition to the Privacy Act, 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)?

**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

**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?

N/A

**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

**External Information Sharing Chart**

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

External Recipient's Name			
Purpose of the Sharing PII Shared			
Content of Applicable Routine Use/Citation to the SORN			
Applicable Statutory or Regulatory or Restrictions on Information Shared			
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 <b>PII</b> )			
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 <b>PII</b> )			
Method(s) Used to Transfer <b>PII</b> (e.g., paper/ oral disclosures/magnetic disk/portable device/email fax/other (please describe if other)			

All individuals that receive PII or drug testing samples are employees and/or contractors of BEP.

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

**Section 5.4(l)**  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))?

## 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?

OPM/GOVT-5 Recruiting, Examining, and Placement Records

OPM/GOVT-10 Employee Medical File System Records

Treasury .015 General Information Technology Access and Accounts Records

### 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

Section 6.2(a)  Yes  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)?

Section 6.2(b)  Yes  No  N/A Does the project or system involve a new collection of information in identifiable form for 10 or more persons from outside the federal government?

Section 6.2(c)  Yes  No  N/A Did the project or system complete an Information Collection Request ("ICR") and receive OMB approval?

The DFFWP involves collecting PII and drug testing samples from employment applicants that are considered "members of the public" until they become active federal employees. As part of BEP's efforts to automate paper documentation into electronic form, DFFWP Managers enter the PII on employment applicants into the eCCF after it is obtained from Human Resources personnel performing employment suitability and onboarding processing and the individual undergoing drug testing. The eCCF data originates from the multi-copy Department of Health and Human Services CCF, which is covered by OMB Control Number: 0930-0158.

## 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?

- GRS 2.1 Employee Acquisition Records, Items 050 and 151, Job Vacancy Case Files

Item 050 - DAA-GRS-2017-0011-0001 – Records of one-time competitive and Senior Executive Service announcements/selections. Temporary. Destroy 2 years after selection certificate is closed or final settlement of any associated litigation; whichever is later.

Item 051 - DAA-GRS-2017-0011-0002 - Records of standing register competitive files for multiple positions filled over a period of time. Temporary. Destroy 2 years after termination of register.

- OPM/GOVT-5, Recruiting, Examining, and Placement Record System of Records are maintained for varying lengths of time, ranging from a few months to 5 years, e.g., applicant records that are part of medical determination case files or medical suitability appeal files are retained for 3 years from completion of action on the case. Most records are retained for a period of 1 to 2 years. Some records, such as individual applications, become part of the person's permanent official records when hired, while some records (e.g., non-competitive action case files), are retained for 5 years. Some records are destroyed by shredding or burning while magnetic tapes or disks are erased.

- GRS 2.7 Employee Health and Safety Records, Items 090, 091, 100, 110, 120, and 130, Employee Assistance Program (EAP) Counseling Records

Item 090 – DAA-GRS-2017-0010-0014 – Records Related to Employee Performance or Conduct. Temporary. Destroy once employee has met condition(s) specified by agreement or adverse action or performance-based action case file has been initiated.

Item 091 - DAA-GRS-2017-0010-0015 - Records Not Related to Performance or Conduct. Temporary. Destroy 7 years after termination of counseling for adults or 3 years after a minor reaches the age of majority, or when the state-specific statute of limitations has expired for contract providers subject to state requirements, but longer retention is authorized if needed for business use.

Item 100 - DAA-GRS-2017-0010-0016 – Employee Drug Test Plans, Procedures, and Scheduling Records. Temporary. Destroy when 3 years old or when superseded or obsolete.

Item 110 - DAA-GRS-2017-0010-0017 - Employee Drug Test Acknowledgment of Notice Forms. Temporary. Destroy when employee separates from testing-designated position.

Item 120 – DAA-GRS-2017-0010-0018 – Employee Drug Testing Specimen Records. Temporary. Destroy 3 years after date of last entry or when 3 years old, whichever is later.

Item 130 – DAA-GRS-2017-0010-0019 - Employee Drug Test Results – Positive Results. Temporary. Destroy when employee leaves the agency or when 3 years old, whichever is later.

Item 131 – DAA-GRS-2017-0010-0020 - Employee Drug Test Results – Negative Results. Temporary. Destroy when 3 years old.

- OPM/GOVT-10, Employee Medical File System Records are maintained for the period of the employee's service in the agency and is then transferred to the National Personnel Records Center for storage, or as appropriate, to the next employing Federal agency. Other medical records are either retained at the agency for various lengths of time in accordance with the National Archives and Records Administration's records schedules or destroyed when they have served their purpose or when the employee leaves the agency. Within 90 days after the individual separates from the Federal service, the EMF is sent to the National Personnel Records Center for storage. Destruction of the EMF is in accordance with General Records Schedule-2.7. Records arising in connection with employee drug testing under Executive Order 12564 are generally retained for up to 3 years. Records are destroyed by shredding, burning, or by erasing the disk.
- 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.

## 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? The SA&A is contingent on the completion of this PLCIA. The ATO will be granted upon completion.

### **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. BEP limits access to the DFFWP Administrators (users) in the Office of Security (Washington, DC Facility) and the Security Division (Forth Worth, TX Facility) that perform drug testing activities and CIO System Administrators.

### **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)?

There is a privacy risk associated with using SSNs for drug sample verification purposes. BEP mitigates this risk by developing a manual process to acquire Human Resource Employee Identification Numbers that will be used as replacements for the SSN until system modifications occur during the next production phase. This change will reduce the number of individuals that gain access to employee/applicant SSNs during drug testing operations.

### **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?

There are no external connectivity associated with the DFFWS. The system automates the multi-copy CCF form, which will be faxed to a secure facility or transferred via email using Federal Information Processing Standard Publication 140-2 ( FIPS 140-2) certified encrypted web-based connections.

#### 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?

<< Space for Narrative Explanation of the Answer to Section 6.4(f): Privacy and/or civil liberties risks presented and mitigation efforts >>

#### 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 conducts periodical audits of all IT systems in order to monitor user activity and to ensure that data is not exposed to unauthorized individuals. DFFWS 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?

The DFFWS is an internally-developed application used to automate paper processes. The application is not accessible by the general BEP workforce or members of the public. BEP conducts an assessment at the procurement or developmental stage 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 of 1973. 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.

### 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?

Recruiting, Examining, and Placement Records

#### 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)?

N/A.

**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// (1/16/2019)

---

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