# Department of the Treasury
# BUREAU OF ENGRAVING AND PRINTING

# Electronic Police Operations Command Reporting System (520131-EPOC)

# BEP Form 2599 – Offense/Incident Report

**April 4, 2017**

## Contact Information

| | |
|---|---|
| **System/Project Name** | Electronic Police Operations Command Reporting System (EPOC) |
| **OMB Unique Identifier** | N/A |
| **FISMA Number** | N/A |

| **1. Who is the person completing this document?** | |
|---|---|
| **Name / Title** | Scott Graf, Security Analyst |
| **Office/Division** | Office of Critical Infrastructure & IT Security (OCIITS), IT Audit and Compliance Division (ITAC) |
| **Phone Number** | (202) 874-3578 |
| **Email Address** | Scott.Graf@bep.gov |

| **2. Who is the system owner?** | | |
|---|---|---|
| **Name / Title** | Troy High, Chief | Thomas Klug, Manager |
| **Office/Division** | DCF Office of Security | WCF Security Division |
| **Phone Number** | (202) 874-4020 | (817) 847-3927 |
| **Email Address** | Troy.High@bep.gov | Thomas.Klug@bep.gov |

| **3. Who is the system manager for this system or application?** | | |
|---|---|---|
| **Name / Title** | Roger Gross, Deputy Commander | Michael Kenny, Inspector |
| **Office/Division** | Police Operations Division | Police Services Branch |
| **Phone Number** | (202) 874-0854 | (817) 847-3944 |
| **Email Address** | Roger.Gross@bep.gov | Michael.Kenny@bep.gov |

| **4. Who is the Information System Security Manager who reviewed this document?** | |
|---|---|
| **Name / Title** | Michael Pease, Chief |
| **Office/Division** | Office of Critical Infrastructure and IT Security (OCIITS) |
| **Phone Number** | (202) 874-2651 |
| **Email Address** | Michael.Pease@bep.gov |

| **5. Who is the Office/Bureau Privacy Officer who reviewed this document?** | |
|---|---|
| **Name / Title** | Anthony Johnson |
| **Office/Division** | Office of Critical Infrastructure & IT Security (OCIITS) IT Audit and Compliance Division (ITAC) |
| **Phone Number** | (202) 874-2258 |
| **Email Address** | Anthony.Johnson@bep.gov |

| **6. Who is the IT Reviewing Official?** | |
|---|---|
| **Name / Title** | Lisa Powe , Manager |
| **Office/Division** | Office of Critical Infrastructure & IT Security (OCIITS) IT Audit and Compliance Division (ITAC) |
| **Phone Number** | (202) 874-0003 |
| **Email Address** | Lisa.Powe@bep.gov |

## A. System Application/General Information

1. **Does this system contain any PII? [ ] No [X] Yes**

2. **What is the purpose of the system/application?**

   The Bureau of Engraving and Printing (BEP) Washington DC Eastern Currency Facility (DCF) - Office of Security, Police Operations Division (OS) and the Western Currency Facility (WCF), Office of Manufacturing Support WCF – Security Division, Police Services Branch (OMS), collectively known as the BEP police, will use the Electronic Police Operations Command Reporting System (EPOC) and the Offense/Incident Report (BEP Form 2599, 2599-1, 2599-2) to collect and store personally identifiable information (PII) of BEP employees, contractors, and members of the public when performing investigations of criminal and administrative incidents and/or general complaints and concerns reported to the BEP police. The word "investigation" for purposes of this PIA does not refer to the "background/suitability investigations" conducted on applicants, employees, and contractors.

   The EPOC system creates an automated web-based repository for forms associated with incidents and investigations. It allows authorized users to query information, prepare management reports, and also allows users to retrieve the status of a particular incident investigation. Although EPOC does not alleviate paper forms or processes, it automates transactions involving paper files, logs, and records.

3. **What legal authority authorizes the purchase or development of this system/application?**

   40 U.S.C. § 1315, 31 U.S.C. § 321, 5141, and Treasury Order 101-33, Delegation of Authority to the Directors, Bureau of Engraving and Printing and United States Mint, to Appoint Special Police Officers, dated March 30, 2010.

4. **Under which SORN does the system operate? (Provide name and number)**

   Treasury/BEP .048, Electronic Police Operations Command Reporting System (EPOCRS), 78 Fed Reg. 22604 (April 16, 2013). This SORN will be amended to modify the "categories of records", "retrievability", and "record source category" sections. In addition, the name of the SORN will be changed to Police Operations Command Reporting System to describe accurately the records contained in the system, which includes the existing paper-based file system and the new IT system (i.e. EPOC).

   The Offense/Incident Report is being modified to include a Privacy Act Statement and a Controlled but Unclassified Information marking.

## B. Data in the System

1. **What categories of individuals are covered in the system? (e.g., BEP employees, contractors, and individuals from the public, other)**

   The category of individuals covered in the EPOC system are BEP employees, contractors, employees of other Federal, State, or local agencies or law enforcement agencies, service company employees, visitors, and members of the public involved in an incident or offense in the areas under the jurisdiction of the BEP Police or that have provided information or evidence to the BEP police during a law enforcement activity and/or investigation.

2. **What are the sources of information in the system?**

   a. **Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other sources?**

      The information contained in the system originates from the individual and/or parties involved directly or indirectly in the incident and their authorized officials and/or legal representatives. Individuals will provide the information in paper forms and/or in-person interviews. The BEP police propose to gather information for the system from appropriate federal, state, and local law enforcement agencies that may have information pertaining to the investigation.

      The BEP Forms used by the BEP police are:

      1) BEP Form 2421- Evidence/Property Custody Record;
      2) BEP Form 2580- Consent for Search of Bureau of Engraving and Printing's Employees and Contractors;
      3) BEP Form 9090 - Security Violations;
      4) BEP Form 9093 - Voluntary Statement; and
      5) BEP Form 2472 – Traffic Accident Report.

      EPOC will generate BEP Form 2599 - Offense/Incident Report, BEP

      Form 2599-1 - Offense/Incident Report - Continuation Sheet, and BEP Form 2599-2 (Supplemental Report).

   b. **What Federal agencies are providing data for use in the system?**

      A wide variety of Federal agencies will provide data in the course of an investigation. The primary source of information will be the U.S. Department of Justice (DOJ), Federal Bureau of Investigations (FBI) Criminal Justice Information Services (CJIS) Division, National Crime Information Center (NCIC), which provides access to numerous databases including the Law Enforcement National Data Exchange and the FBI Law Enforcement Online (LEO) Web Portal. In addition, the Police Divisions from the Department of the Treasury and its bureaus such as the Office of the Inspector General, the Treasury

Inspector General for Tax Administration (TIGTA), the Internal Revenue Service (IRS), the U.S Mint, and the Bureau of Alcohol Tobacco, Firearms, and Explosives (ATF) could also provide data for use in the system.

**c. What state and/or local agencies, tribal governments, foreign governments, or international organizations are providing data for use in the system?**

BEP may receive data for use in the system from state and local agencies that include, but are not limited to the District of Columbia, Washington Metropolitan Police Department (MPD) and the State of Texas, Department of Public Safety (TxDPS). BEP may receive law enforcement incident and investigation data from other federal, state, or local agencies, it receives its information from two primary databases in use by MPD & TxDPS:

- Washington Area Law Enforcement System (WALES); and
- Texas Law Enforcement Telecommunications System (TLETS).

There are no automated interfaces between BEP EPOC and other law enforcement databases.

**d. From what other third party sources will data be collected?**

Various third party sources could provide data relevant to an investigation. For example, an insurance company may provide documentation on a vehicle accident claim under investigation to document the monetary impact of an accident.

**e. What information will be collected from employees, government contractors and the public?**

The BEP police will request significant information from the BEP employees, BEP contractors, and members of the public involved in an investigation related to an incident and/or general complaint reported to the BEP police. EPOC and BEP Form 2599, 2599-1, and 2599-2 (Offense/Incident Report) will record the following information:

I. Information about Incident:

- Type of Report;
- Report Number/Case Number;
- Narrative Description of Incident;
- Date and Time of Call;
- Incident Type;
- Incident Sub-Type;
- Location (Name, Address, Building, Room, Floor, Other);
- Jurisdiction;
- Dispatched Officer's Name;

- Dispatch Date/Time;
- Arrival Date/Time;
- Date/Time Cleared;
- Date and Time Occurred;
- Day of Week Occurred;
- Date and Time Reported;
- Day of Week Reported;
- Disposition Condition;
- E-mail Recipient (BEP police);
- E-mail Address (BEP police);
- Active Directory Group;
- Comments;
- Mode of Info; and
- NCIS/Wales Check.

II. Individual Identification and Contact Information for Involved Individuals:

- Type of Person (Victim, Suspect, Witness);
- Name (Last name, First name, Middle initial);
- DOB;
- Place of Birth;
- Age;
- SSN (provided voluntarily);
- Gender (Male, Female, or Other);
- Description (Race, Height, Weight, Hair Color, Eye Color, Scars, Marks and Tattoos and location);
- Description of clothing worn (i.e., hat, coat, shirt, pants, skirt, shoes, glasses etc.);
- Address (Number, Street, Apartment Number, City, State, Country, and Zip Code);
- Telephone (Home, Business);
- Injured (Y/N);
- Passport Info (Number, Country of Issue, Expiration Date); and
- SACS Badge Number (BEP User ID).

III. Information about Suspect Status:

- Suspect Status; Status (Not Identified, Government Employee, Government Contractor, Not related to the Government, Arrested, Not Arrested;
  Citation # Issued, 9090-1 Number Issued, Released);
- Suspect Disposition;
- Issued Number;
- Narrative;

- Assigned By;
- Assigned Date;
- Comments;
- Reporting Official's Name;
- Reporting Official's SACS Badge Number;
- Reporting Official's Signature (Paper Form only.);
- Date of Signature;
- Supervisor's Name;
- Supervisor's Signature (Paper form only);
- Date of Signature;
- Recommendations (Open Investigation, Process Citation, 9090-1, No Further Action);
- Investigation Opened (Y/N);
- Case Number;
- Referred to (Text Field);
- Closed (Text Field);
- Suspect Developed/Arrested (Y/N);
- Property Recovered (Y/N);
- Court Date (Y/N) Text Field; and
- Entered NCIC (Yes, No, N/A).

IV. Information about Driver's License:

- Name (Last, First, Middle);
- Physical Address (City, State, Country, Zip Code);
- Number;
- Issuing State;
- Expiration Date; and
- Status (Active, Revoked, Suspended, No OL).

V. Information about Vehicle, Owner, Description, Licensing and Insurance:

- Owner's Name (Last, First, Middle);
- Owner's Address (City, State, Country, Zip Code);
- Vehicle Description (Make, Model, Year, Color);
- Registration (License Number, Year, State, VIN);
- Insurance Information (Name Address and Telephone number of Insurance Carrier);
- Insurance Policy Number; and
- Expiration Date of Insurance Policy.

VI. Information about Property:

- Item;

- Brand Name;
- Model;
- Serial Number;
- Ownership (Government or Personal);
- Quantity;
- Color;
- Estimated Value;
- Property was (Secured Unsecured); and
- Status of Property (Missing, Recovered, Partially Recovered).

VII. Information about Other Agency Involvement:

- Name of Other Involved Agencies;
- Notified Time; and
- Arrived Time.

VIII. Information about Evidence:

- Evidence Sized (Y/N/Tag Number);
- Type of Evidence Sized;
- Evidence Storage Location;
- Other Agency Case Number;
- Receiving Component;
- Address of Component;
- Location;
- Person Evidence Received From (Last Name, First Name, MI, Title);
- Check Box (Owner/Other);
- Location from Where Obtained;
- Reason Obtained;
- Date/Time Obtained;
- Item Number;
- Quantity;
- Full Description Text;
- Comments; and
- Reporting Official Comments.
-

IX. Continuation Fields:

In addition to the fields listed above, EPOC has the capability to provide additional free text data on any listed data element.

X. Attachments:

Any report acquired in the course of the investigation can be appended to the individual's record in EPOC. Examples of the potential attachments are:

- BEP Form 9093, Voluntary Statement;
- BEP Form 9090, Security Violation;
- BEP Form 2421, Evidence/Property Custody Record;
- BEP Form 2472, Traffic Accident Report;
- BEP Form 2580, Consent for Search of Bureau of Engraving and Printing's Employees and Contractors;
- Medical Information;
- Insurance Claims;
- Police Reports from other Law Enforcement Agencies;
- Statements provided by individuals;
- Digital Images captured during the incident or investigation;
- Audio and Video images or recordings captured during the incident or investigation; and
- Any other reports pertinent to the incident and/or complaint.

As listed above, the EPOC will also contain identifying information of the BEP police conducting an investigation such as the Employee ID Number, SAC Badge Number, or PIV Badge Number.

**3. Accuracy, Timeliness, and Reliability**

**a. How is data collected from sources other than from Treasury records going to be verified for accuracy?**

The BEP police will verify the information for accuracy with the individual and the paper-based files. The data obtained from other law enforcement agencies will be verified with the originating agency and the individual. Record data will also be verified through additional manual identity checks of the FBI Integrated Automated Fingerprint Identification System (IAFIS) when needed and before reports are finalized.

**b. Is completeness required? [] No [X] Yes**

**c. What steps or procedures are taken to ensure the data is current and not out-of-date?**

The BEP police will request the individual to provide voluntarily a form of identification to verify that the information provided is accurate. If the individual refuses to provide any form of identification, the data name element will be captured in the incident record as Jane or John Doe. The additional IAFIS check when needed, serves as a step or procedure to ensure that the data is current.

**d. Are the data elements described in detail and documented? If yes, what is the name of the document? [ ] No [X] Yes**

The data elements are described in detail and documented in the EPOC Design Document.

## C. Attributes of the Data

1. **Is the use of the data both relevant and necessary to the purpose for which the system is being designed?**

   Yes. The data is needed by the BEP Police to perform law enforcement activities/ investigations of incidents that occur in the areas under the jurisdiction of the BEP police.

2. **Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed? [] No [X] Yes**

   External data on an individual (such as data from NCIC or agencies participating in investigations) may be added to or combined with system data and stored in the system. Resulting data could create a broader information profile on an individual than previously available with either independent data set. The data is stored as an electronic record within EPOC and associated with a specific incident.

3. **Will the new data be placed in the individual's record? [] No [X] Yes**

   The data is stored in the record established for a specific incident identified with a Report Number/Case Number.

4. **Can the system make determinations about employees/members of the public that would not be possible without the new data?**

   Yes. The record will establish a link between an individual and the incident that generated the record.

5. **How will the new data be verified for relevance and accuracy?**

   The PII contained in the system originates from the individual and/or external database systems. The identity of an individual will be verified with a form of identification provided voluntarily by the individual. Data obtained from external database systems will be verified with the originating agency. A supervisor will review any additional data entered into the IT system by the BEP police for accuracy. Record data will also be verified through an internal multi-step internal workflow process before reports are finalized.

6. **If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**

Physical, technical, and administrative safeguards as described in section D.7 below protect the data.

**7. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.**

Physical, technical, and administrative safeguards as described below protect processes and prevent unauthorized access.

1) Physical Safeguards

EPOC servers can only be accessed using a BEP workstation connected to the BEP network. BEP is considered a secure building. EPOC is not connected to any external database system.

2) Technical Safeguards

Logical access to EPOC requires an approved user to present a Personal Identifiable Verification (PIV) card along with their associated Personal Identification Numbers (PIN). The approved user is then allowed access based on their role, which is associated with pre-defined permissions. Users are assigned to an access level based on their roles. This mitigates the risk of a user being granted permissions above what is required to perform job functions.

3) Administrative Safeguards

An enterprise access control policy addresses the roles, responsibilities, and compliance issues. The policy specifies that access controls shall provide protection for confidentiality, integrity, and availability. In addition, BEP establishes conditions for group membership, identifies users of the EPOC system, requires appropriate approvals for requests to establish accounts, and grants access to the information system based on: i) a valid access authorization; ii) intended system usage; and iii) other attributes as required.

The various roles associated with the EPOC are described in the EPOC documentation. The established BEP IDAM process is used to request, review, and grant access to these roles.

**8. How will the data be retrieved? Is the data retrieved by a personal identifier? If yes, explain and list the identifiers that will be used to retrieve information on the individual.**

EPOC data is stored in the system associated with a specific incident, which could be identified by an Offense/Incident Report Number/Case Number. The following data elements may be used to retrieve the data in the system:

- Name;
- DOB;
- SSN;
- Passport Number;
- Incident Report Number/Case Number;
- Date and Time of Incident;
- Location of Incident;
- Report Status; and
- Name of BEP police Assigned.

**9. What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

EPOC will produce an Offense/Incident Report (BEP Form 2599, 2599-1, 2599-2) that will contain the individuals' names and other identifying information, contact information, property information, voluntary statements, photographs, and/or investigative activity summaries. The BEP police intend to use the Incident Report to disclose information to appropriate third parties such as law enforcement agencies responsible for investigating and prosecuting the violation of, enforcing, or implementing a statute, rule, regulation, order, or license.

Reports may be disclosed to BEP personnel based on their need-to-know to perform job functions.

## D. Maintenance and Administrative Controls

**1. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

Authorized personnel from the DCF's Office of Security and WCF's Security Division have access, with read and write privileges to the data based on their assigned roles. Some information is limited to BEP police supervisors associated with the specific incident. System Administration personnel from IT can access all data.

**2. What are the retention periods of data in the system?**

Records are managed in accordance with National Archives and Records Administration approved BEP Records Schedule (N1-318-11-1), Item 12 (N1/318/04/8) or General Records Schedule GRS 18. .

**3. What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**

Paper records approved for destruction in accordance with applicable NARA approved BEP Record Schedule are destroyed by shredding or maceration. Records in electronic

media approved for destruction in accordance with applicable NARA approved BEP Record Schedule are electronically erased using accepted techniques.

The procedures used to facilitate this process are documented in the BEP Circular No. 80-05, Records Management Program (2006); BEP Circular No. 80-05.3, Records Storage (2007); and BEP Circular No. 80-05.4, Policies and Procedures for Electronic Records and Email (2006).

The BEP police and CIO Directorate are responsible for ensuring that records are preserved, records no longer of current use are promptly destroyed, and retention schedules are implemented and that the BEP complies with the recordkeeping requirements issued by the Department of the Treasury, National Archives and Records Administration, Office of Management and Budget, and the National Institute of Standards and Technology.

4. **Is the system using technology in ways the office or bureau has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)? If yes, explain.**

   No.

5. **How does the use of this technology affect public/employee privacy?**

   EPOC automates existing manual processes and makes information storage and retrieval faster and more efficient. EPOC provides the ability to correlate law enforcement information to find potential relationships between criminal investigations, crime incidents, and other law enforcement information.

6. **Will the system provide the capability to identify, locate, and monitor individuals? If yes, explain.**

   Yes. EPOC captures information specifically with the intent of identifying an individual.

7. **What kind of information is collected as a function of the monitoring of individuals?**

   N/A.

8. **What controls will be used to prevent unauthorized monitoring?**

   N/A.

9. **Under which SORN does the system operate? (Provide name and number)**

   EPOCRS operates under Treasury/BEP .048, Electronic Police Operations Command Reporting System (EPOCRS), 78 Fed Reg. 22604 (April 16, 2013).

**10. If the system is being modified, will the SORN require amendment or revision? Explain.**

Yes. The SORN will be amended to modify the "categories of records", "retrievability", and "record source category" sections. The BEP police intend to collect new information that is not part of the "categories of records" and will use external database systems as a "record source category". In addition, the BEP police intend to retrieve records based on new PII fields. Lastly, the name of the SORN will be changed to Police Operations Command Reporting System to describe accurately the records contained in the system, which includes the existing paper-based file system and the new IT system.

## E. Access to Data

**1. Who will have access to the data in the system? (e.g., contractors, users, managers, system administrators, developers, others).**

Authorized personnel of DCF's Office of Security and WCF's Security Division collectively known as the BEP police will have access to this data based on their assigned roles. IT personnel including managers, administrators, and system engineers will have restricted access to privacy information.

**2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?**

Access to the electronic and paper -based files is determined by pre-authorized privileges granted to users based on their need- to- know to perform daily job functions.

The standard Identity Manager, System Access Request process (former BEP Form 8392) is used to review personnel requests to interface with the system and to assign approved users to specific roles. Access to the data is determined by User ID and password verification and role assignment. The responsibilities and access to data for the individual users is dictated by the role they are assigned.

Users are placed into groups based on their roles and job functions.

**3. Will users have access to all data on the system or will the user's access be restricted? Explain.**

Authorized personnel from the DCF's Office of Security and WCF's Security Division have access, and read and write privileges to the data based on their assigned roles. Some information is limited to BEP police supervisors associated with the specific incident. System Administration personnel from IT can access all data.

**4. What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? List procedures and training materials.**

Users participate in mandatory Annual Privacy Awareness Training sponsored by the Department of the Treasury, Office of Privacy and Civil Liberties (OPCL) and the Records Management-Employees and Contractors Training sponsored by the Department of the Treasury, Office of Privacy, Transparency, and Records (OPTR).

Authorized users are granted restricted access based on user roles and need- to- know.

5. **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system?**

   Contractors are involved with the design, development, and maintenance of the EPOC. Contractors are required to complete Annual Privacy Awareness Training sponsored by OPCL and the Records Management-Employees and Contractors Training sponsored by OPTR.

6. **Do other systems share data or have access to the data in the system? If yes, explain.**

   No.

7. **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

   The Chief of the Office of Security - Police Operations Division (DCF) and the Manager of the Office of Manufacturing Support - Security Division, Police Services Branch (WCF).

8. **Will other agencies share data or have access to the data in this system?**

   Yes.

   **[X] Federal [X] State [X] Local [ ] Other**

9. **How will the data be used by the other agency?**

   These records may be used to disclose information to:

   - Appropriate federal, state, and local agencies responsible for investigating or prosecuting the violation of, or for enforcing or implementing, a statute, rule, regulation, order, or license, where the disclosing agency becomes aware of a potential violation of civil or criminal law or regulation;
   - A court, magistrate, or administrative tribunal, in the course of presenting evidence, including disclosures to opposing counsel or witnesses, for the purpose of civil discovery, litigation, or settlement negotiations or in response to a court order, where relevant or potentially relevant to a proceeding, or in connection with criminal law proceedings;

- A congressional office in response to an inquiry made at the request of the individual to whom the record pertains;
- Representatives of the National Archives and Records Administration (NARA) who are conducting records management inspections under authority of 44 U.S.C. 2904, 2906;
- The U.S. Department of Justice (''DOJ'') for its use in providing legal advice to the Department or in representing the Department in a proceeding before a court, adjudicative body, or other administrative body before which the Department is authorized to appear, where the Department deems DOJ's use of such information relevant and necessary to the litigation, and such proceeding names as a party or interests: (a) The Department or any component of it; (b) Any employee of the Department in his or her official capacity; (c) Any employee of the Department in his or her individual capacity where DOJ has agreed to represent the employee; or (d) The United States, where the Department determines that litigation is likely to affect the Department or any of its components;
- Appropriate agencies, entities, and persons when (a) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

**10. What are the procedures that allow individuals to access their information?**

EPOC maintains records that are covered by the SORN listed in Section 9 above. Individuals seeking notification of and access to any record contained in these systems of records, or seeking to contest its contents, may submit a request in writing to the BEP Disclosure Officer, whose contact information and submission instructions can be found at https://www.moneyfactory.gov/foia.html under "How to File a FOIA (Freedom of Information Act) FOIA Request" or "How to File a Privacy Act of 1974 Request."

You may send your FOIA or PA request by:

1. **Mail:**

Disclosure Officer
Bureau of Engraving and Printing
Office of the Chief Counsel-FOIA and Transparency Services
14th & C Streets, SW, Room 419A
Washington, D.C. 20228-0001

2. **Fax:** (202) 874-2951

3. **Department of the Treasury's FOIA Online Portal.** CLICK HERE TO ACCESS TREASURY'S FOIA ONLINE

The BEP does not accept or respond to FOIA/PA requests by email. Please remember to include your signature if you decide to file your FOIA/PA request by mail or fax.

**11. Who is responsible for assuring proper use of the data?**

Chief, Office of Security (DCF) and Manager, Security Division (WCF).

**The Following Officials Have Approved This Document**

1. **System Owner**

   **Name: Troy High (DCF)** **Thomas Klug (WCF)**

2. **System Manager**

   **Name: Richard Wilcox (DCF)** **Michael Kenny (WCF)**

3. **Information System Security Manager**

   **Name: Michael Pease**

4. **Government Information Specialist (Privacy)**

   **Name:**

5. **IT Review Official**

   **Name: Lisa Powe**

6. **Deputy Assistant Secretary for Privacy and Treasury Records (when necessary)**

   **Name:**