Department of the Treasury
BUREAU OF ENGRAVING AND PRINTING

Manufacturer Cash Handling Equipment (MCHE) (330111-MCHE)

January 16, 2015

B. System Application/General Information

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

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

   The BEP Office of Product Development (OPD) uses the Manufacturer Cash Handling Equipment (MCHE) IT system to store contact information of approved Banknote Equipment Manufacturers (BEM) and Currency Reader Manufacturers (CRM) eligible to receive new designs and production samples of Federal Reserve Notes (FRN) for purposes of updating their products to denominate and/or authenticate genuine currency. BEM and CRM are considered BEP-Approved upon satisfactory completion of a background investigation performed by the BEP-Office of Security (OS). The OS notifies the OPD the name of the approved BEM and CRM and contact information of the BEM and CRM liaison.

   The purpose of the database is to create a list of all BEM and CRM approved to receive FRN for testing purposes. This list will facilitate communication between OPD and BEM/CRM liaisons. MCHE allows users to generate several reports. These reports provide details associated with the companies dealing with FRN.

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

   5 U.S.C. §301, 31 U.S.C. §321.

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

   MCHE contains PII from the public but does not retrieve records by any PII.

C. Data in the System

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

   The BEM/CRM liaison and BEP employees and contractors are covered in the MCHE system.

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 source of the information is from the BEM/CRM liaison. The liaison provides the information in the BEP Background Investigation Form used by the BEP-Office of Security.

In addition, the system captures information about OPD personnel responsible for adding the BEM and CRM data into the system. For example, actions taken by the OPD personnel are captured in the audit logging system along with their User ID.

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

No Federal agency is providing data for use in the MCHE system.

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

No state and/or local agencies, tribal governments, foreign governments, or international organizations are providing data for use in the system.

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

Data is not collected from any third party source.

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

MCHE collects information from approved BEMs and CRMs. The information collected from the public and BEP employees and contractors include:

e.1) Company name and address;
e.2) Name of liaison and his/her company's phone number;
e.3) Company's fax number;
e.4) Liaison's company email address;
e.5) Liaison's title within the company; and
e.6) Name of the BEP employee or contractor using the system, the actions performed by these individuals on the system such as update or delete, and the date the action was performed.

3. Accuracy, Timeliness, and Reliability

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

A background investigation is conducted to validate the data provided.

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 BEM/CRM is required to update their information when changes occur to ensure that it is current and not out of date.

d. **Are the data elements described in detail and documented? [ ] No [X] Yes**

If yes, what is the name of the document?

The data elements are documented in the Manufacturer Cash Handling Equipment IT System.

D. 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 use to facilitate communication between the BEP and BEM/CRM that have been approved to receive bank notes for testing purposes.

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? [X] No [ ] Yes**

The system will not derive new data or create previously unavailable data about an individual through aggregation.

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

N/A. No new data is derived.

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

N/A. No new data derived.

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

N/A. No new data is derived.

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

N/A. Data is not being consolidated.

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

   N/A. Processes are not being consolidated.

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.**

   A filter describes a data element or range that is used to query the data and extract information. The BEM/CRM data is retrieved by:

   - Company Name
   - City (Company Site)
   - Country (Company Site)
   - Series (Relates to the FRNs being examined)
   - Denomination (Relates to the FRN being examined)
   - Dates (Range of dates associated with a record)
   - Test Site (Is site identified as a Test Site)
   - Security Agreement (Does Site have a Security agreement)
   - NDA (Does Site have a NDA)
   - BEP Restrictions (Does Site have any BEP Restrictions in place)
   - Security Visitation (Has Site had a Security Visit)
   - Security approved (Is site approved)

   MCHE has been modified to remove the capability to use the liaison's name to access the data. There is no longer a capability to access the data using PII.

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

   MCHE allows users to generate the following reports:

   - Details Report: This report generates company names and their sub-sites along with their location.
   - Cash Handling Equipment Manufacturer (CHEM) Report: This report is similar to the information generated in the Details Report but in a different format.
   - Security Visitation Report: This report generates name and location of company, if and when the company was visited, and if the site is approved by BEP to receive notes for testing purposes.
   - Audit Review Report: This report allows authorized users to review audit records for up to 3 years. This report captures the identity of the user, the action the user performed, such as update or delete, and the date the action was performed.

The reports are generated as needed. The Details Report is sent to the Lead for the Vendor Outreach Program at the Currency Technology Office (CTO), Federal Reserve Bank of Richmond, upon their request. The Vendor Outreach Program Lead requests the report in an effort to maintain a current list of companies approved to test bank notes.

The Details Report, CHEM Report, and the Security Visitation Report contain the name, work e-mail address, and work phone number of the BEM/CRM liaison.

E. 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?**

   The MCHE application is only operated at the Eastern Currency Facility (ECF).

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

   Records are retained and disposed in accordance with BEP Records Schedule No. 7.1, Administrative Services Program Files.

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 for disposal are shredded and electronic records are permanently deleted, in accordance with 36 C.F.R. § 1226.24. Reports will be retained and disposed in accordance with BEP Records Schedule 7.1, Administrative Services Program Files. Procedures are documented in BEP Circular 80-05, Records Management Program, dated December 18, 2006, and BEP Circular 80-05.4, Policies and Procedures for Electronic Records and Email, December 18, 2006.

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?**

   N/A

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

   Yes.

The system captures the name and identifying information of the approved BEM/CRM liaison. (Note, there may be more than one liaison for each BEM/CRM). This would provide the capability to identify but not locate or monitor the liaison.

The MCHE also requires each BEP employee or contractor to be identified and authenticated prior to granting access. After access is granted, audit controls are in place to monitor user activities during their session.

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

   N/A. The system does not monitor the BEM /CRM liaison officers.

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

   The system implements the following controls to safeguard against unauthorized monitoring:

   a. Access Controls: Individuals are granted least privileges based on their roles and need-to-know.
   b. Audit Controls: User activities are monitored on the system.
   c. MCHE users complete mandatory annual privacy awareness training.

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

   MCHE contains PII from the BEM /CRM liaison but does not retrieve records by any PII. A SORN is not required.

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

    A SORN is not required. The modification to MCHE includes:

    a. The Web server, BEPWEBP1, running IIS v6.0 upgraded to Web server, BEPWEB02DMPWP, running IIS v7.5;
    b. The Database server, BEPSQL01, (SQL 2005) to Database server, BEPCLUDMPWP, (SQL 2008 R2);
    c. Upgrade from a 3.5 .Net Framework to a 4.0 .Net Framework.
    d. Additional sub-sites field;
    e. Last security inspection date field added; and
    f. Removing the ability to filter by name of individual.

F. Access to Data

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

IT personnel such as, the system administrator and employees, and contractors in OPD.

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

   Users must complete BEP System Access Request Identity Manager Form requesting access to the system and be approved for access by an authorized BEP personnel. Users are granted access based on their roles and need-to-know. Criteria, procedures, controls, and responsibilities regarding access to the system are documented in the access control portion of the MCHE system security plan.

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

   Users are granted restricted access base on their roles and need-to-know.

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 the 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).

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 system.

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

   There is no electronic sharing of the data. However, the Vendor Outreach Program Lead at the Currency Technology Office (CTO), Federal Reserve Bank of Richmond will have access to the printed Details Report.

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

   Chief, Office of Product Development.

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

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

   The Vendor Outreach Program at the Currency Technology Office (CTO), Federal Reserve Bank of Richmond will have access to the Details Report referenced in section

D9. The CTO of the Federal Bank of Richmond requires the data in the Details Report because the United States Secret Service only authorizes CTO to work with companies and company representative who have been vetted through the BEP-approval process and the Details Report provides notice of this process.

BEMs and CRMs are aware that the information is shared with the CTO. They are verbally notified of this fact during BEM/CRM conference presentations and during the application process to become a BEM or CRM.

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

The CTO requests reports in an effort to maintain a current list of companies approved to test bank notes.

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

Chief, Office of Product Development