Privacy Impact Assessment

Name of System:

National Electronic Incident Reporting System (NEIRS)

Purpose of the System:

The Protection Department seeks to improve its incident management capabilities by implementing a centrally managed solution that will:

- Support the collection, management, and sharing of information regarding reported incidents on or related to United States Mint property, property for which the United States Mint shares jurisdiction through a Cooperative Agreement, Memorandum of Understanding or other arrangement, or property or assets under United States Mint custody or control.
- Be usable by all United States Mint Police officers and units in accordance with applicable procedures.
- Improve data management and security. .
- Provide a tracking system to notify supervisors of case status.

System of Record Number(s), if applicable at this time: A System of Record Notice will be prepared and published following completion of this Privacy Impact Assessment.

A. Contact Information: *(Provide name, title, and organization.)*

1. ***Who is the person(s) completing this document?***
   Don Meyerhoff (Branch Chief, Policy and Training, United States Mint Police)

   Who is the system developer/analyst? Michael Iacangelo, Program Analyst Information Technology Department/Program Management Branch.

   Who is the system owner/manager? Chief, United States Mint Police.

2. ***Who is the Information Systems Security Manager who reviewed this document?*** Chris Carpenter, Division Chief, Information Security

3. ***Who is the Bureau Privacy Act Officer who reviewed this document?***

   Kathleen Saunders-Mitchell, Disclosure Officer

B. System Application/General Information:

1. ***Does this system contain any personal information about individuals?***
Yes. While the system is generally organized by incident and not by individual, it contains personal information on individuals searchable by individual or by identifier.

2. ***What legal authority authorizes the purchase or development of this system/application? (List statutory provisions or Executive Orders that authorize the maintenance of this information to meet an official program mission/goal.)***

40 U.S.C. § 1315; 31 U.S.C. § 321, under which the Secretary of the Treasury issued Treasury Order 101-33 (March 30, 2010), which re-delegated that authority to the Director of the Mint; Pub.L.104-208, div. A, title I sec. 101(f) (title V, sec.517) (Sept. 30, 1996), 110 Stat. 3009-314, 3009-346 *codified at* 31 U.S.C. 5141 (note).

3. ***For new systems, how is privacy addressed in documentation related to system development; including statement of need, functional requirements analysis, alternatives analysis, feasibility analysis, benefits/cost analysis, and especially the initial risk assessment?***

Privacy will be addressed in system documentation by:

- Specifying and complying with applicable public law and policy;
- Deploying effective electronic role-based security procedures and access rules built into system programming;
- Referencing (and enforcing) bureau user rules and Information Technology departmental policy;
- Creating (and enforcing) United States Mint Police operating procedure reflecting system use procedures and privacy practices; and
- Requiring training for system users.

C. ***<u>Data in the System:</u>***

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

Employees, contractors, visitors and other members of the general public involved in incidents on or related to United States Mint property, property for which the United States Mint Police share jurisdiction through a Cooperative Agreement, Memorandum of Understanding or other arrangement, or property or assets under United States Mint custody or control.

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

- Interviews with employees, contractors and general public who are involved in incidents,

- The National Crime Information Center ("NCIC") database, Treasury Office of Inspector General, and other federal, state or local law enforcement agencies conducting investigations they or the United States Mint initiate.

2a. Is the source of the information the individual or is it taken from another source? If not directly from the individual, then what other sources?

Information may be collected directly from the individual interviewed, from witnesses (which may include other United States Mint employees), from the Treasury Office of the Inspector General, NCIC database, or from federal, state or local law enforcement agencies.

2b. What Federal agencies are providing data for use in the system?

Depending on the incident, the United States Mint may work with other agencies on investigations it or another agency initiates. The United States Mint may use and store in the system information obtained during such investigations. Agencies that provide such data may include Treasury components (such as Treasury Office of the Inspector General, Treasury Inspector General for Tax Administration and the Bureau of Engraving and Printing) and outside agencies (such as the Department of Justice, Federal Bureau of Investigations, General Accountability Office, and the Department of Homeland Security.

2c. What State and/or local agencies are providing data for use in the system?

Various state and local agencies contributing indirectly through the NCIC database, and district attorney's offices, state and local police/investigative agencies where United States Mint facilities and interests are located.

2d. From what other third party sources will data be collected? n/a

2e. What information will be collected from the employee and the public? (e.g., social security numbers, addresses, telephone numbers, badge numbers, user identifiers, credit card numbers, etc.)

The United States Mint may collect and store some or all of the following information relating to individuals:

- Contact information such as name, address, and phone numbers;
- Driver's licenses and dates of birth;
- Property descriptions, vehicle and license plate numbers;
- Medical information (typically in the case of accidents or injuries)

- Investigation information, social security numbers and physical descriptions.

3. Accuracy, Timeliness, and Reliability

3a. How will data collected from sources other than from bureau records be verified for accuracy?

The bureau will seek corroboration of individual's statements. Data obtained from the NCIC will be verified with the originating agency. Record data will also be verified through a multi-step workflow process before reports are finalized.

3b. How will data be checked for completeness?

Record data will be checked for completeness through the multi-step workflow process before reports are finalized.

3c. Is the data current? How will this be ensured?

Record data will be updated and verified through the multi-step workflow process before reports are finalized.

3d. Are the data elements described in detail and documented? If yes, what is the name of the document?

Yes. *"Requirements - United States Mint Police National Electronic Incident Reporting System."*

4. What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of information (other than required or authorized uses)?

This depends on the circumstances. Generally, if the individual's interaction with the United States Mint Police is voluntary, then (other than providing mandatory identification for access to United States Mint buildings) that individual is not obligated to provide information to the United States Mint Police.

However, if the nature of the interaction between the individual and the United States Mint Police is or becomes related to enforcement of law or to the safety and security of people and property, providing the information may not be voluntary. All information provided to the United States Mint Police in connection with incidents on or related to United States Mint property, property for which the United States Mint Police share jurisdiction (through a Cooperative Agreement, Memorandum of Understanding or other arrangement), or property or assets under United States Mint custody or control will be

subject to the Privacy Act and to the Privacy Act exceptions and routine uses applicable to the data.

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. Data is used to document incidents and their investigations.

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?***

   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. Accuracy and relevance of the data will be verified through workflow review.

3. ***Will the new data be placed in the individual's record?***

   Yes, if accurate and relevant.

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

   Final determinations (such as decisions to refer matters to law enforcement agencies, the Department of Justice or the Treasury Office of Inspector General) may be supported by or based in part on compiled data.

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

   Accuracy and relevance will be verified through supervisory workflow.

6. ***Do the records in this system share the same purpose, routine use, and security requirements?***

   Yes.

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

The application will have role-based and location-based access controls, workflow rules and audit capabilities to support these controls. Departmental policy, operating procedures and directives will also govern data access and use.

Access by the public to the information contained within NEIRS will be governed by the Privacy Act and the Freedom of Information Act (FOIA) process, including exemptions and exceptions where applicable. Data within the system may be subject to certain classification, such as "For Official Use Only" or "Law Enforcement Sensitive" if applicable criteria are met.

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

While the system is generally organized by incident and not by individual, it contains personal information on individuals searchable by individual or by identifier. The database may be searched by any of its fields or by word search, including individual names, driver's license numbers, and SSN to the extent they have been inserted into the database. The data may also be searched and retrieved by:

- officer assigned
- date;
- individual name, social security number, driver's license number or any other information described in 2(e) above;
- activity code;
- location; and
- status

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

Reports that may be generated by the system are expected to include incident and investigative reports (which may contain individuals' names and other identifying information, contact information, property information, statements, and photographs) and investigative activity summaries (brief summaries of the foregoing).

Expected uses of these reports include:

- Documentation of incidents for internal recordkeeping, and reference where relevant to employee management; and
- Documentation and communication of information to parties such as Treasury Office of the Inspector General, United States Attorney, state and local District Attorneys and law enforcement agencies for whom the information is relevant to incidents or investigations in which they are involved.

Reports and their contents may be disclosed to United State Mint Police and United States Mint managers in accordance with applicable internal procedures and the Privacy Act, and authorized investigatory and law enforcement personnel and others in accordance with the Privacy Act including exceptions and routine uses.

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 system is tied to a dedicated central database. This database is centrally managed, secured and maintained behind the United States Mint firewall system.

2. ***What are the retention periods of the data in this system?***
   The records will be maintained and disposed in accordance with a media neutral United States Mint records retention schedule for the NEIRS system approved by National Archives and Records Administration.

3. ***What are the procedures for disposition of the data at the end of the retention period?***
   The records will be maintained and disposed in accordance with a media neutral United States Mint records retention schedule for the NEIRS system approved by National Archives and Records Administration.

4. ***Is the system using technologies in ways not previously employed (e.g., monitoring software, Smart Cards, Caller ID)?***

   Not at this time.

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

   The system is not using previously unused technologies at this time

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

   Yes, to the extent it can record an individual's address, other contact information and physical descriptions. However, the system itself cannot monitor an individual.

7. ***What kinds of information are collected as a function of the monitoring of individuals?***

The system itself does not monitor individuals. Relevant information on individuals obtained through authorized law enforcement activities may be stored in the system.

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

Commencement of any investigation using information on individuals in the system requires approval from, at a minimum, the Chief of the United States Mint Police, and may also require approval of the Treasury Inspector General and/or federal, state or local law enforcement agencies.

9. ***If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors?***

The system is not constructed to be accessed by the public.

10. ***Under which Privacy Act system of records notice does the system operate?***

This is a new system. We expect to prepare and file new System of Record notice for this system.

11. ***If the system is being modified, will the Privacy Act System of Records Notice require amendment or revision? Explain.***

This is a new system.

F. ***Access to Data:***

1. ***Who will have access to the data in the system? (e.g., users, managers, contractors, others) Will those with access to the data have appropriate training and security clearances to handle the sensitivity of the information?***

Access to the database itself is expected to be limited to United States Mint Police and Information Technology staff providing application and system support, and is subject to further role and location-based controls. United States Mint employees are subject to security clearances and receive training on the Privacy Act, applicable user rules, operating procedures, policies and directives, and system operations. Information technology contractor staff members have contractual security and Privacy Act training requirements, security clearances, and nondisclosure agreements.

System data and reports containing system data may be disclosed to United States Mint Police, United States Mint managers and others under certain circumstances consistent with the Privacy Act, as described in the response to D.9 above.

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

   Access will be governed by role-based and location-based electronic access controls in the application, applicable operating procedures, bureau policies and directives, the requirements of contracts and contractor employee nondisclosure agreements, and by the Privacy Act. Physical security measures govern access to servers on which the data is stored.

   Information Technology personnel providing services in connection with the system will have undergone clearances and will sign non-disclosure agreements prior to working with NEIRS and related United States Mint systems.

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

   Access to the system itself is restricted to United States Mint Police and Information Technology personnel providing system support, with further restrictions based on roles and locations. United States Mint Police Headquarters command staff and Information Technology system support staff will have access to all the data in the system, but read/write controls will govern data modification by all personnel. Reports containing system data may be provided to United States Mint managers and others in accordance with the Privacy Act (including exceptions and routine uses) and with other applicable law and policy.

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

   Role-based and location–based user access and restrictions and read/write/review controls will be built into the system's design. Audit functions will also help monitor and identify unauthorized use. Applicable directives, operating procedures, and United States Mint electronic system user rules will govern access to and use of information contained within the database.

5. ***Are contractors involved in the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?***

   Contractors are involved in the customization and maintenance of the system. Privacy Act clauses and other security compliance requirements are included in their contracts.

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

   There is no automated data interface between the NEIRS system and other systems through which data is shared.

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

   There is no such shared interface.

8. ***Will other agencies share data or have access to the data in this system (Federal, State, Local, Other)?***

   Entities that may have access to data in the system in accordance with applicable United States Mint procedures and applicable law include Treasury Office of the Inspector General; United States Attorney; state and local District Attorneys; and international, federal, state and local law enforcement agencies for which the information is relevant to incidents or investigations in which they are involved.

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

   In connection with authorized law enforcement activities and other activities in accordance with applicable law.

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

    - Chief, United States Mint Police;
    -United States Mint Police Command personnel, Field Chiefs, and Supervisory Police Officers;
    -United States Mint Office of Information Security;
    -Command staff of outside agencies to which data is provided

The Following Officials Have Approved this Document:

1. *System Owner*

10/16/12

(Signature and Date)

Name: Dennis P. O'Connor Title: Chief, United States Mint Police

2. *Program Manager*

10-16-12

(Signature and Date)

Name: Don Meyerhoff Title: Branch Chief, Policy and Training, United States Mint Police

3. *Information Systems Security Manager*

10-19-12

(Signature and Date)

Name: Chris Carpenter Title: Division Chief, Information Security

4. *IT Reviewing Official*

(Signature and Date)

Name: Michael Iacangelo Title: Project Manager

5. *Records Management Officer*

10/19/12

(Signature and Date)

Name: Yvonne Pollard *Title: Brach Chief, Compliance, ISD*

6. Privacy Act Officer

(Signature and Date)
Name: Kathleen Saunders-Mitchell *Title: Disclosure Officer*