Department of Energy
Privacy Impact Assessment (PIA)

Name of Project: Federal Bureau of Investigations Billing System
Bureau: Department of Energy
Project Unique ID: 019-10-01-22-02-3028-00
Date: 02/08/2008

A. CONTACT INFORMATION

1) Who is the person completing this document?

Joanne Csordas (HS-1.21), Office of Business Operations, Office of Resource Management, Office of Health, Safety and Security, U.S. Department of Energy, HS-1.21, 1000 Independence Avenue, SW, Washington D.C. 20585, (301) 903-3573

2) Who is the system owner?

Joanne Csordas (HS-1.21), Office of Business Operations, Office of Resource Management, Office of Health, Safety and Security, U.S. Department of Energy, HS-1.21, 1000 Independence Avenue, SW, Washington D.C. 20585, (301) 903-3573

3) Who is the system manager for this system or application?

Raymond Holmer (HS-1.22), Director, Office of Information Management, Office of Resource Management, Office of Health, Safety and Security, U.S. Department of Energy, HS-1.22, 1000 Independence Avenue, SW, Washington D.C. 20585, (301) 903-7325

4) Who is the IT Security Manager who reviewed this document?

Vincent Le (HS-1.22), Office of Information Management, Office of Resource Management, Office of Health, Safety and Security, U.S. Department of Energy, HS-1.22, 1000 Independence Avenue, SW, Washington D.C. 20585, (301) 903-4648

5) Who is the Privacy Act Officer who reviewed this document?

Kevin Hagerty, Director, Office of Information Resources, U.S. Department of Energy, MA-90, 1000 Independence Avenue, S.W., Washington, DC 20585, 202-586-8037.

B. SYSTEM APPLICATION/GENERAL INFORMATION

1) Does this system contain any information about individuals? Yes

a. **Is this information identifiable to the individual?** [1] Yes

b. **Is the information about individual members of the public?** Yes

c. **Is the information about DOE or contractor employees?** Yes.

2) **What is the purpose of the system/application?** The purpose of this application is to monitor, record, and authorize payment of billings provided by the Federal Bureau Investigation (FBI) for conducting background security investigations.

3) **What legal authority authorizes the purchase or development of this system/application?** Title 42, United States Code (U.S.C.), Section 7101 et. seq.; 50 U.S.C. 2401; Title 10, Code of Federal Regulations (CFR), Part 710, subparts A and B; Executive Orders (E.O.) 10450 and 12968; 5 CFR Part 732; DOE Order 470.4 "Safeguards and Security Program dated August 26, 2005; Personnel Security Manual DOE M 470.4-5 dated August 26, 2005; and Director of Central Intelligence Directive 1/14 dated January 22, 1992.

C. DATA IN THE SYSTEM

1) **What categories of individuals are covered in the system?** Individuals who require a security clearance with the Department of Energy (DOE).

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?** The source of information is provided by the applicant and the FBI.

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

c. **What tribal, state, and local agencies are providing data for use in the system?** None.

---

[1] "Identifiable Form" - According to the OMB Memo M-02-22, this means information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptor).

d. **From what other third party sources will data be collected?** None.

e. **What information will be collected from the individual and the public?** Information collected includes the following: Name, bill number, date of bill, submittal date of the investigation, field site, case type, and case price.

3) **Accuracy, Timeliness, and Reliability**

a. **How will data collected from sources other than DOE records be verified for accuracy?** Data accuracy is verified by the applicant and the data owners who provide or enter the data into the system.

b. **How will data be checked for completeness?** The data/system owner reviews the data for completeness.

c. **Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date?** Yes, the data is current and the financial data is updated periodically to report current status.

d. **Are the data elements described in detail and documented?** Data elements are described and documented in the System Security Plan.

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 relevant to monitor, record, and authorize payment to the FBI for conducting security background 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?** No the system will not derive new data.

3) **Will the new data be placed in the individual's record?** N/A

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

5) **How will the new data be verified for relevance and accuracy?** N/A

6) **If the data are being consolidated, what controls are in place to protect the data from unauthorized access or use?** The data is not being consolidated.

7) **If processes are being consolidated, do the proper controls remain in place to protect the data and prevent unauthorized access?** Yes.

8) **How will 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.** Data is retrieved by a search function using an individual name and/or other data fields described in question #2e above.

9) **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?** Only financial reports associated with billing and payment for security investigations conducted by the F BI. These reports are used for the budget planning and operational spending purposes. System owner and backup personnel are authorized access to the system. Financial reports are provided to cognizant program managers for billing and verification purposes.

10) **What opportunities do individuals have to decline to provide information (e.g., where providing information is voluntary) or to consent only to particular uses of the information (other than required or authorized uses)?** The data is required to process and obtain a DOE security clearance. The information is provided voluntarily.

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?** No, the system is not operated at other sites.

2) **What are the retention periods of data in the system?** Data retention procedures are in accordance with General Records Schedule 7 "Expenditure and Accounting Records." This information can be obtained at http://www.archives.gov/records-mgmt/ardor/grs07.html.

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?** Data retention procedures are in accordance with General Records Schedule 7 "Expenditure and Accounting Records." This information can be obtained at http://www.archives.gov/records-mgmt/ardor/grs07.html. The reports will be kept for 6 years and 3 months after the close of the fiscal year involved.

4) **Is the system using technologies in ways that DOE has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?** No.

5) **How does the use of this technology affect public/employee privacy?** N/A

6) **Will this system provide the capability to identify, locate, and monitor individuals?** No the system does not have the ability to identify, locate or monitor individuals.

7) **What kinds of information are 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 Privacy Act system of records notice does the system operate?** DOE-18 "Accounting Financial System."

10) **If the system is being modified, will the Privacy Act system of records notice require amendment or revision?** No, the system is not being modified.

F. ACCESS TO DATA

1) **Who will have access to the data in the system?** Only the system owner, designated backup personnel, and the system administrator are authorized to access the data.

2) **How is access to the data by a user determined?** User identification and password are required to authenticate authorized users.

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

4) **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?** Users are required to follow the security procedures described in the system security plan and the DOE Orders related to information protection. Annual security refresher briefing is provided to users.

5) **Are contractors involved with 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 included in their contracts and other regulatory measures addressed?** Yes. Contractors were involved with the design and development of the system and will be involved with the maintenance of the system. Information may be disclosed to contractors and their officers and employees in performance of their contract. Individuals provided this information are subject to the same limitation applicable to DOE officers and employees under the Privacy Act, 5 U.S.C. 552a.

Pertinent contract language states that data covered by the Privacy Act may be disclosed to contractors and their officers and employees. Any information that is obtained or viewed shall be on a need-to-know basis. Contractors are required are required to safeguard all information they may obtain in accordance with the provisions of the Privacy Act and the requirements of DOE. The contractor shall ensure that all documents and software processed, and the information contained therein, are protected from unauthorized use and mishandling by assigned personnel.

6) **Do other systems share data or have access to the data in the system? If yes, explain.** No, other systems do not share or have access to the data.

7) **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?** N/A

8) **Will other agencies share data or have access to the data in this system?** No, other agencies do not share or have access to the data in this system.

9) **How will the data be used by the other agency?** N/A

10) **Who is responsible for assuring proper use of the data?** N/A

The Following Officials Have Approved this Document

1) **System Manager**

_____ (Signature) 6/11/08 (Date)
Name: Raymond Holmer
Title: Director, Office of Information Management, Office of Health, Safety and Security

2) **Privacy Act Officer**

_____ (Signature) 6/13/08 Date)
Name: Kevin T. Hagerty
Title: Director, Office of Information Resources, Office of Management

3) **Senior Privacy Official**

_____ (Signature) 6-13-08 (Date)
Name: Ingrid A.C. Kolb
Title: Director, Office of Management