Financial Management Service
Privacy Impact Assessment

Name of Project: BICMAN
Project's Unique ID: BICMAN

Once the Privacy Impact Assessment (PIA) is completed and the signature approval page is signed, please provide copies of the PIA to the following:

- FMS IT Security Manager
- FMS AC-area Privacy Act Liaison

Also refer to the signature approval page at the end of this document.

For purposes of completing any FMS PIA, "data" means any information on an individual in identifiable form, i.e., any information that can be used to identify an individual.

A. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals?

Yes.

2) What is the purpose of the system/application?

BICMAN does not represent a new collection of information, but rather, serves as a repository for all background investigations, adjudications and security clearance data regarding FMS employees, applicants for employment and contractors. The acronym BICMAN stands for Background Information Case Management system.

BICMAN contains the results of background investigations conducted primarily by the U.S. Office of Personnel Management. The Department of Defense and other federal investigative agencies also provide background investigations. Routine checks during the background investigation process include Federal Bureau of Investigation checks, Immigrations and Naturalization Service checks and Credit Reports which are stored. The actual copies of the credit reports are not stored within BICMAN. Routine law enforcement check results from state and local agencies are typically captured during the investigation process.

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

The statutory authority for the Personnel Security function within the Security

Division can be found in Executive Order 10450, Executive Order 12968, Treasury Order (TO) 102-12, and TO 12-32.

B. DATA in the SYSTEM:

1) What categories of individuals are covered in the system?
FMS employees, applicants for employment and contractors are covered in BICMAN.

2) What are the sources of the 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 source?
Individuals provide information directly by completing security questionnaires, SF-85, SF-85P, or SF-86 and other paperwork required to schedule their background investigation. Additional information is captured from the employee or contractor during the background investigation.

b. What Federal agencies are providing data for use in the system?
The OPM background investigation could contain information from OPM, FBI, Defense Department, and other federal agencies, but not in every instance.

c. What State and local agencies are providing data for use in the system?
The OPM background investigation contains routine responses from state law enforcement agencies such as the Maryland State Police, county level law enforcement agencies, and possibly city law enforcement agencies.

d. From what other third party sources will data be collected?
Equifax, Inc. credit reporting agency.

e. What information will be collected from the employee and the public?
No information is collected from the public. FMS Employees/Applicants/Contractors provide information required to conduct a background investigation. This involves completing Questionnaires for National Security positions (SF-86), or Questionnaires for Public Trust positions (SF 85P) and Non Sensitive positions (SF-85), and other paperwork needed to schedule their background investigation.

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than FMS records be verified for accuracy?
There is no independent verification of information provided by federal

agencies such as OPM, FBI, and DOD.

b. How will data be checked for completeness?
The completed response from the federal agency is assumed to be complete and accurate.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

OPM relies on other federal agencies to provide current and up to date information when conducting the Background Investigation.

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

C. <u>ATTRIBUTES OF THE DATA:</u>

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

Absolutely, the completed background investigation information is necessary to grant security clearances, and make suitability judgments for employment at FMS.

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?

BICMAN is a central repository of information from other sources. BICMAN does not create previously unavailable data.

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

N/A

4) Can the system make determinations about employees/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, no new data

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

Access to BICMAN data is restricted to FMS Security Division personnel with a need to know only. Division personnel are granted access to BICMAN through the FMS LAN only.

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

   N/A

7) **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.

Yes, a personal identifier retrieves the data. Data can be retrieved by first name, last name, or last four (4) digits of the social security number.

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

A written summary of the information developed during the background investigation is developed by personnel security specialists in the division. The reports are used in making a final determination for hiring an applicant, allowing a contractor to work at FMS, denying an employee or contractor to work at FMS, and granting a security clearance.

The reports can be accessed by Security Division personnel with BICMAN access. FMS employees with a need to know such as Labor Relations and Policy Branch, Office of Chief Counsel, or Treasury OIG representatives can see the summary reports. OPM investigators conducting background investigations can also see the summary reports.

9) **What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent.)**

Providing information to initiate their background investigation is voluntary. However, not providing the minimum information to conduct their background investigation would probably preclude them from working at FMS. Individuals sign release forms in the standard forms used granting consent to conduct their background investigation.

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?

BICMAN is only operated from the Security Division.

2) What are the retention periods of data in this system?

The data contained in BICMAN is being retained indefinitely.

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?

No data contained in BICMAN has been disposed of. Any reports generated from the background investigation are stored in hard copy of the security folder within the FMS Security Division. The security folder is maintained throughout the duration of employment, and for 5 years after an employee, contractor or applicant separates. Five years after separation, the files are destroyed in accordance with FMS Records and Information Management Branch policies.

4) Is the system using technologies in ways that the FMS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?
N/A

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? If yes, explain.
No.

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 systems of records notice does the system operate? Provide number and name.

A system of records (SOR) entitled “Treasury/FMS.007 – Personnel Security System” is listed in the Federal Register, Volume 67, and Number 33 and applies for the system.

10) **If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**

No. If the application is modified to enhance functionality or add a data field, it would not change the nature of the privacy act information.

E. ACCESS TO DATA:

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

Access to the BICMAN application data is restricted to FMS Security Division employees. See D.9 above for other personnel who could see hard copy reports generated from BICMAN.

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

The application system administrators grant access to BICMAN. There are 3 levels of access; view, normal and system administrator. The least necessary privilege concept is used. Users are given access only to the extent necessary to perform functions of their job assignments.

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

User access is determined by the application system administrators. Access is restricted to the level of user privileges determined by the application system administrators. All users are restricted form seeing their own information.

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

Prior to granting access and during training, all users are required to read and sign an application specific Rules of Behavior Form. Users of the BICMAN system are advised they are accessing sensitive personal information covered under provisions of the Privacy Act of 1974. Unauthorized disclosure of personal information or data may be illegal and punishable under applicable Federal laws. Users are also advised of the audit log capability built into the application. Any change made to the data base is documented within the application and identifies what user made the change, the date and time of the change, and what information was changed to. Users are trained that the application system administrators can review the audit log at anytime.

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 inserted in their contracts and other regulatory measures addressed?

Contractors developed the application and continue to provide maintenance.

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?**

N/A.

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

Other agencies do not have access to the application. See D.9 above for other personnel who could view hard copy data from the system if reviewing a security folder.

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