USFA
Admissions System Rehost Project
Major Application

Privacy Impact Assessment

9/28/2004

Privacy Impact Assessment

Table of Contents

Introduction

The objective of the privacy impact statement (PIA) is to assist the Department of Homeland Security (DHS)/Emergency Preparedness and Response (EP&R) Directorate/Federal Emergency Management Agency (FEMA) staff to identify and address information privacy requirements when planning, developing, implementing, and operating individual agency information management systems. The PIA is a new government requirement that is to be used when evaluating whether existing statutory requirements and key information management concepts and requirements are being applied to new and modified systems that contain personal information. These requirements are drawn from the Privacy Act of 1974, as amended, 5 U.S.C. 552a, Public Law 93-579; Computer Security Act of 1987, Public Law 100-235; Clinger-Cohen Act of 1996, Public Law 104-106; Paperwork Reduction Act of 1995, 44 U.S.C. 3501, et seq., as amended; Freedom of Information Act, 5 U.S.C. 552 (2000); and Office of Management and Budget (0MB) Circulars A-130: Management of Federal Information Resources (1996) and A-123: Management Accountability and Control (1995). A template developed by the National Institute for Standards and Technology was used to develop the analysis.

The PIA process also helps to identify sensitive systems so that appropriate information assurance measures are in place such as secured storage media, secured transmission and access controls.

The goals accomplished in completing a PIA include:

Providing senior FEMA management with the tools to make informed policy and system design or procurement decisions based on an understanding of privacy risk, and of options available for mitigating that risk.

- Ensuring accountability for privacy issues with system project managers and system owners.
- Ensuring a consistent format and structured process for analyzing both technical and legal compliance with applicable privacy law and regulations, as well as accepted Privacy Act policy.
- Providing basic documentation on the flow of personal information within FEMA systems for use and review by policy and program staff, systems analysts, and security analysts.

Personal Information

Personal information is information about an identifiable individual that may include but is not limited to:

- Information relating to race, national or ethnic origin, religion, age, marital or family status;

- Information relating to education, medical, psychiatric, psychological, criminal, financial, or employment history;
- Any identifying number, symbol or other particular assigned to the individual; and name, home telephone number, fingerprints, blood type, or DNA.

Scope

The scope of the analysis is to evaluate the type of data stored by the FEMA United States Fire Administration, National Emergency Training Center (NETC) Management Operations and Support Services Division Admissions System with respect to privacy concerns. Access controls and storage protection of any data element considered privacy-sensitive is assessed and reported within this document.

In order to comply with the guidance contained in Office of Management and Budget Memorandum M-03-22 (2003), the analysis should address the following areas:

1. What information is to be collected;
2. Why the information is being collected;
3. Intended use of the information;
4. With whom the information will be shared;
5. What opportunities individuals have to decline to provide information;
6. How the information will be secured; and
7. Whether a system of records is being created under the Privacy Act, U.S.C. 552a.

In addition, the analysis should identify the choices FEMA made regarding an IT system or collection of information as a result of performing the PIA. This, as well as the seven items above, will be addressed in the responses to the questions and the information below.

The system being analyzed was developed initially in 1982 to accommodate the vast amount of documents and information associated with the admissions and registration process at the FEMA NETC. From the beginning, an effort was made to collect only the information needed to process applications for admissions and the associated travel expense reimbursement and housing. There are a few items of information being requested that are normally collected by educational institutions for statistical purposes. Providing this information has always been voluntary and the information provided cannot be used in determining eligibility for a course. Since certain information being collected was protected by the Privacy Act, special precautions have been taken related to the handling, storage, and access to the information. These precautions include controlling access to the work area where the information is being handled, controlling release of reports that contain Privacy Act protected information, controlling access to the automated system that contains the student information, and controlling the release of any student information in the system. These precautions have been utilized since the early 1980's. The system was moved from a mainframe environment to a file server environment in the late 1980's. In the late 1990's, an effort was initiated to rehost the

system from FoxPro to Oracle, which is the FEMA standard software for large databases, and from a DOS to a Windows platform. Certain upgrades were being incorporated in the system including the ability to performance certain functions using the web. These functions include being able to apply for courses on-line, being able to check the status of an application or a student stipend reimbursement on-line, being able to access certain reports, and being able to import files for courses delivered by state and local fire and emergency services training agencies. These new functions caused the need to conduct a Privacy Impact Assessment. They also caused the need for additional security measures described below to protect the information in the system. When an individual wants to check the status of an application or a stipend, certain information known to the individual and contained in the system must be used to access that information. Every effort has been and will continue to be made to protect the information in the system.

Privacy Questions

Data in the System

1. Generally describe the information to be used in the system.
   The system contains information from individuals who have applied for courses offered by FEMA's National Fire Academy (NFA) or the Emergency Management Institute (EMI), certain personal financial information from accepted students so that electronic payments can be made under the student stipend reimbursement program, and information on non-students (contract instructors and special guests) that utilized housing accommodations on the campus.

2.a. What are the sources of the information in the system?
   The source of the applicant information is FEMA Form 75-5, General Admissions Application or shorter form versions of that application, and the on-line application which contains the same fields as the paper application. Supplemental information may also be requested for specific courses or programs. The source of the financial information is FEMA Form 75-3, Student Stipend Agreement and the source of information for accommodations is FEMA Form 75-10, Request for Housing Accommodations. All three forms as well as the electronic version of the application contain Privacy Act statements. Student information can also be provided from course instructors and fire and emergency management training systems using floppy disks and electronic transmission through a web module. The information provided by the states is the same that is collected on an application. FEMA Forms 75-5 and 75-10 have been assigned report control numbers by OMB.

   b. What databases are used?
   Within the admissions system, one database containing several tables is used. The system does not utilize any external databases outside the admissions system; however, it does import data from training systems including student information from individuals who have taken NFA courses conducted by state and local training agencies.

   c. What Federal Agencies are providing data for use in the system?
   Information used in the system is provided by applicants, accepted students, or non-student special groups. The data would be provided by students applying for NFA

or EMI courses and representing state and local government, volunteer organizations, private industry, foreign governments, and the Federal government. Unless the applicant is representing a Federal agency, no Federal agencies are providing data for use in the system.

d. What state and local agencies are providing data for use in the system?
The majority of individuals applying for courses are from the fire service or emergency management community. The information is provided by the individuals rather than their sponsoring agencies. Data is provided by State or local training systems for NFA or EMI courses conducted by them.

e. What other third party sources will data be collected from?
No data will be collected from other third party sources.

f. What information will be collected from the applicant?
The applicant indicates citizenship (city and country of birth for non-U.S. citizens), social security number or an alternate number that has been assigned in lieu of the social security number, name, mailing address, work phone number, alternate phone number, fax number, email address, course code and title, course location, dates requested, course pre-requisite as described in the course catalog, special assistance request, name and address of the organization being represented, fire department identification number, current position and years in that position, jurisdiction type, type of work for the organization, organization type, employment status, number of staff in the organization, size of population served by the organization, brief description of the activities or responsibilities as they relate to the course for which they are applying, primary responsibility and type of experience, number of years of experience, date of birth, sex, ethnicity and race, signature of the applicant, and required concurrences or approvals. If the accepted student is applying for a stipend, the individual provides their name, business phone number, mailing address, name of the financial institution, bank routing number, account title, account number, and type of account on the Student Stipend Agreement. Other than the financial institution name and account information, the information is generated by the admissions system and pre-printed on the stipend form for the student. Information such as age, sex, and ancestral heritage are collected for statistical purposes only. Personal information is provided on a voluntary basis; however, failure to provide certain information may delay processing the application because there may be insufficient information to determine eligibility for the course. The social security number is necessary because of the large number of individuals who have identical names and birthdates and whose identities can only be distinguished by the social security number. The social security number is used for recordkeeping purposes, i.e., to ensure that the academic record is maintained accurately. Disclosure of the social security number is voluntary. If the social security number is not provided, a unique identifier will be assigned so that the application can be processed. Use of a unique identifier in lieu of the social security number will create difficulty in providing a complete and accurate academic record. The information collected is used to determine eligibility for a particular class for which the applicant is applying based on the selection criteria for that course.

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

The data is not verified. FEMA would defer to the individual and that the personal information provided by each individual applicant is accurate. The information in the system is updated each time an applicant applies for a course.

b. How will data be checked for completeness?
The application is reviewed prior to entering the data into the system. Applications that are incomplete in terms of providing information in the required fields are returned to the applicant with a letter indicating what other information is needed to process the application. When applicants are able to apply for courses on-line, completion of certain fields will be required. The application cannot be submitted until all the required fields are completed.

c. Is the data current? How do you know?
The data is updated each time an individual applies for a course or information is received electronically. There is an audit feature in the system to indicate when a record was last updated and by whom.

4. Are the data elements described in detail and documented? If yes, what is the name of the document?
Yes, the data elements are described in detail and documented in the requirements documents for the various modules of the system along with other documentation that has been developed as part of the development process. There is also a data dictionary and schema, along with requirements documents for the various system interfaces.

Access to the Data

1. Who will have access to the data in the system (Users--Managers, System Administrators, Developers, Other)?
There will be no general access to the data for anyone who is not authorized to work with the data as part of their routine duties. Privacy Act protected data is only available to individuals working in the NETC Admissions and Housing Offices. Organizational information is available to program offices and the general public. No reports containing Privacy Act protected information are made available outside the NETC admissions and housing work areas. Access to information is controlled by passwords, access rights to the system and by security levels within the system. Individuals applying for courses electronically are only permitted to input information. Individuals can electronically check the status of an application or stipend reimbursement provided they have the information necessary to access that report. When an applicant signs the admissions application, they authorize the release of certain information.
2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?
Access to the data is controlled by a “need to know” the information in the performance of official duties such as entering applications or stipends, updating data in the system, or responding to inquiries, and tightly controlled by the system administrator. Access is provided based on the duties and responsibilities of individual’s official position related to the course admissions process. An admissions specialist assigns access rights.

3. Will users have access to all data on the system or will user access be restricted? Explain.
   There are various levels of users with access based on official duties on a "need to know" basis. Individuals who work in the NETC admissions or housing work areas will have access to the modules of the system that they need in order to perform their official duties. Program offices will have access to reports that do not contain any Privacy Act protected individual information. System users are required to provide their user name and password to obtain access. Authentication is part of the process for controlling access. Access to the various part of the system is based on rights granted and is controlled by the System Administrator and the Senior Admissions Specialist.
4. What controls are in place to prevent the misuse (e.g. browsing) of data by those having access?
   Access to personal data is controlled with access provided only to the staff members that have a "need know" and to have access to specific personal information in the performance of their duties. Contractor work is monitored by government staff and contractor supervisor's to prevent misuse. This is done through a random review to monitor contractor performance and a review of work procedures and processes.
5. a. Do other systems share data or have access to data in this system? If yes, explain.
   There are six other systems that interface with the admissions system. Some of the interfaces, receive data from the Admissions System, others provide data to the Admissions System, and another performs both actions. These interfaces are the MicroPurchase System, State Data Import, EMI Independent Study System, EMI FEMA Employee Knowledge Center, Training Information and Analysis System, and NFA Learning Management System. The MicroPurchase System interface provides information to the Admissions System for contract instructors requiring housing on the campus. The system pulls course/activity information and specific instructor information when housing is needed. The State Data Import interface allows State and local training systems to electronically transmit training information to the Admissions System. Through an interface with the EMI Independent Study System, the Admissions System will have the capability of varying course pre-requisite information for certain EMI resident courses. Information on upcoming training classes will be provided through an interface with the EMI FEMA Employee Knowledge Center. An interface with the Training Information and Analysis System will allow certain admissions information to be reflected in that system. An interface with the NFA Learning Management System will allow individuals completing NFA independent study courses to apply electronically. Through the electronic payment process, certain information is electronically transmitted to the Department of the Treasury so that stipend payments can be made. Some of the information transmitted to Treasury is Privacy Act protected but is necessary to make electronic payments.

   b. Who will be responsible for protecting the privacy rights of the applicants affected by the interface?
   The Admissions system owner is responsible for protecting the privacy rights of applicants. There is no interface of Privacy Act protected information with other systems other than the Treasury system. Only staff members with a "need to know"

an individual's information in the performance of their official duties will have access to Privacy Act protected type of information.

6.a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?
Other agencies will not be sharing data or have access in this system. The only information that will be available from the system will be certain reports that do not contain any Privacy Act protected information. In fact, the reports do not contain any self-identifying information such as the names of individual students, with the exception of the roster report and query capability which provides limited organizational information.

b. How will the data be used by the agency?
The data will be used to determine each applicant's eligibility for courses, provide housing for accepted applicants, provide stipend reimbursement for eligible students, preparing course completion certificates and transcripts, and communicate with applicants and selected students.

c. Who is responsible for assuring proper use of the data?
Everyone in the admissions and housing work areas is responsible for the proper safeguarding and use of the data. The Admissions Specialist monitors use and access by controlling access rights, monitoring contractor performance, and monitoring work processes and procedures.

d. How will the system ensure that agencies only get the information they are entitled to? Access to the data is controlled by security levels using the security administration features in the application software. The system provides access only as approved by the Senior Admissions Specialist. Information, other than what is available to the general public, is not provided to other agencies

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, only information that is needed to determine an individual's eligibility for courses and to process stipend reimbursements is requested with the exception of the date of birth, sex, and race/ethnicity, which is used for statistical purposes at a composite level only. This information is compiled for statistical purposes and does not identify any individuals.

2.a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?
The system will not derive or create any new data about an individual through aggregation.

b. Will the new data be placed in the individual's record?
There will not be any new data created in the student's record.

c. Can the system make determinations about applicants that would not be possible without the new data?
The system only makes determinations on whether or not an individual qualifies for a particular course based on parameters in the system and information provided by the applicant.

d. How will the new data be verified for relevance and accuracy?
New data is not verified since it would be very difficult to verify information from an admissions application. The NETC assumes that the data an individual provides about himself or herself is accurate.

3.a. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?
With the rewriting of the MicroPurchase System, certain demographic data on contractor instructors that was formerly maintained in the MicroPurchase System will now be maintained in the admissions system. The admissions system will continue to receive housing requirements from the MicroPurchase System for contract instructors. This effort will consolidate Privacy Act protected information on contract instructors and eliminate the need to maintain it in two separate systems, reducing the likelihood of unauthorized access or use.

b. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.
The processes are not being consolidated. The MicroPurchase System rehosting effort includes normalizing the data and where it should be properly stored.

4.a. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.
Data on an individual can be retrieved by name or social security number. The social security number is used as a unique identifier since individuals may put their name differently on different applications or there may be more than one individual with the same name and birth date. If an applicant does not provide a social security number, a unique identifier is assigned; however, this may cause difficulty in providing an accurate and complete academic record on an individual.

b. What are the potential effects on the due process rights of applicants of:
   1) consolidation and linkage of files and systems;
   The system and files are not being consolidated or linked.
   2) derivation of data;
   No derivation of data exists.
   3) accelerated information processing and decision making;
   The newer software should process data faster, which will be beneficial to system users. It will not impact the process rights of applicants.
   4) use of new technologies.
   This will not impact on the process rights of applicants.

c. How are the effects to be mitigated?
No effects to mitigate exist.

Maintenance of Administrative Controls

1.a. Explain how the system and its use will ensure equitable treatment of applicants.
The system stores only applicant information. One of the features of the system; however, is that applicants, based on their position and course being applied for, can be automatically qualified for the courses without a physical review of the application. Race/ethnicity, sex, and date of birth information are removed from the application prior to review for qualification. This measure has been taken to

enhance equitable treatment of applicants.

b. 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 will be operated primarily from one site in Emmitsburg, Maryland. There will be an extension of the system at Mt. Weather in Bluemont, Virginia, and at Noble Training Center in Anniston, Alabama, with limited write capability to the database. This will include making changes to to data for students at those respective locations. Only one database will be maintained for the entire system at Emmitsburg.

c. Explain any possibility of disparate treatment of individuals or groups.
No disparate treatment of individuals or groups by the system should occur because the system is not used to determine whether or not an applicant is not qualified for a course. Instead this is done by individual review of applications by contractor staff and with government oversight. The applicant is notified of his/her acceptance or non-acceptance into a course and given the opportunity to provide additional information if they have not been accepted.

2.a. What are the retention periods of data in this system?
The data is retained for an indefinite period at the present time. The documents that are used to provide the input to the system have a retention period of 40 years.

b. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?
If the information on an individual has not been accessed in 3 years, it is placed in a history file, which is still accessible. No data has been eliminated from the system.

c. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?
No requirements exist for determining if the data is still sufficiently accurate, relevant, timely, and complete. Information is maintained in the system so that a transcript can be issued.

3.a. Is the system using technologies in ways that the DHS has not previously employed (e.g. Caller-ID)?
No. In fact, the system is being upgraded and rehosted to utilize Agency-standard software.

b. How does the use of this technology affect applicant privacy?
Among the features of the upgraded and rehosted system is the ability for an individual to apply for courses on-line and to check the status of an application or a stipend reimbursement. Since this provides access to certain data from outside the firewall, measures have been taken in the development of the web application to ensure security of the database and protection of the information in it. Therefore, external customers will not be able to access the database directly.

4.a. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.
The system will not have the capability to identify, locate, or monitor individuals outside the system itself. Individuals can be located within the system through the use of the name or social security number. Individual records, however, will include an audit trail containing the various actions that have taken place in the

system related to the applicant. System operators can locate and identify particular applicants but the system will not do it automatically. There is also a monitoring process for individuals enrolled in the Executive Fire Officer Program. This monitoring involves tracking completion of required research projects.

b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.
It will not automatically do so, unless it becomes necessary for a system operator to perform a custom query of system data to identify individuals from a particular organization such as a fire department or a particular group such as volunteers.

c. What controls will be used to prevent unauthorized monitoring?
Security measures have been put in place so that unauthorized connections to the servers are prohibited. The primary system is behind the FEMA firewall and access is controlled by password and granting of access rights. The web module resides outside the firewall and only contains Privacy Act data that is provided by applicants. This data is sent to a temporary server on a regular basis to reduce the amount of time the data is in a non-secure area. The system does not maintain information outside the firewall. A temporary file server is utilized inside the initial firewall as a holding area until the admissions system calls for that information. The information is downloaded to the admissions system on a regular basis. Information for reports that do not contain Privacy Act protected information and are available to the public is downloaded to the temporary server on a nightly basis.

5.a. Under which Systems of Record notice (SORN) does the system operate? Provide number and name.
The system was created under the Privacy Act and has been designated Systems of Record NETC 017- NETC Admissions System

b. If the system is being modified, will the SORN require amendment or revision? Explain.
Yes, while the system itself is not being modified, the form in which the records will be made available and retrieved will be modified from only hard copy to include electronic form and hard copy. The upgrading and rehosting of the system is consistent with the system of records. There will be a minor revision to the Privacy Act system of records statement on the application to address the new capability for applicants to applying electronically for NFA or EMI courses rather than the previous option of applying only by hard copy paper.

Appendix A

Viewer Privacy and Security Notice, Admissions Wed Module

**********WARNING**********

For site security purposes and to ensure that this service remains available-to-all users, this government computer system employs software programs to monitor host and network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.

Except for authorized law enforcement investigations, no other attempts are made to identify individual users or their usage habits. Raw data logs are used for no other purposes and are scheduled for regular destruction in accordance with National Archives and Records Administration guidelines.

Unauthorized attempts to upload information or change information on this service are strictly-prohibited and may be punishable under the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act.

**********WARNING**********