Privacy Impact Assessment
for the

Independent Study Database (ISDBS)

January 2007

Contact Point
Jennifer Ogle
Independent Study Program COTR
FEMA/EMI
301-447-1585

Reviewing Official

Hugo Teufel III

Chief Privacy Officer

Department of Homeland Security

(571) 227-3813

Abstract

The Emergency Management Institute (EMI) of the Federal Emergency Management Agency (FEMA), an agency of the Department of Homeland Security (DHS), maintains an Independent Study Database that collects and maintains student training completion information, such as individual student data, organizational data, etc. for our Independent Study program. This information is used to create and update student records, track completions and failures and issue completion certificates. Tracking this information is important to the program in order to issue college credit for completion of EMI IS courses, as well as issuing student transcripts to be provided to institutions for helping the student obtain continuing education units and/or to military institutions for military personnel to earn retirement points for successful completion of IS courses. Tracking this information is also important in order to provide training completion data to the State, local, and Tribal emergency management agencies to satisfy their compliance with HSPD-5 and HSPD-8.

Introduction

The Emergency Management Institute (EMI) of the Federal Emergency Management Agency (FEMA), an agency of the Department of Homeland Security (DHS), recognizes the importance of protecting the privacy of students of the EMI, as processed by the Independent Study Database (ISDBS). As mandated by the U.S. Congress, issues of privacy must be taken into consideration when developing or operating automated systems. Privacy protections must be made an integral component of the automated system, and this process is usually implemented by performing a privacy impact assessment (PIA).

The Independent Study (IS) Program is authorized under the Robert T. Stafford Disaster Relief and Emergency Act, Public Law 93-288 as amended. This program supports the DHS mission by providing valuable training via on-line courses to Federal, State, local and Tribal emergency management personnel, as well as the general citizenry of the United States to enable them to better prepare and respond to threats and hazards to the nation. This program allows training to reach vast and diverse audiences without requiring that they attend a resident course at EMI, or at a state-sponsored course which significantly reduces the cost of hosting training and associated travel costs for students. It specifically supports DHS Strategic Objective 4.2 to provide scalable and robust all-hazard response capability as it relates to the National Incident Management System.

The purpose of ISDBS is to collect and maintain student training completion information, such as individual student data, i.e. student name, social security number, mailing information, organizational information, phone number, and course completion date for the Independent Study (IS) Program. The ISDBS also maintains training completion data for the National Incident Management System (NIMS) training courses that are required of all Federal departments and agencies through Homeland Security Presidential Directive 5 (HSPD-5), "Management of Domestic Incidents". This directive also requires that Federal preparedness assistance funding for States, Territories, local jurisdictions and Tribal entities be dependent on NIMS compliance. Training is one of the important elements that State, Territory, local and Tribal entities must complete during FY 2006 and in out years in order to become NIMS compliant. The NIMS training courses are a core part of EMI's Independent Study Program. In order to be able to provide training completion data to the State, local, and Tribal emergency management agencies to satisfy their compliance with HSPD-5 and HSPD-8, it is necessary to collect registration information. The system also issues training completion certificates and transcripts.

Over the last two years, the requirements and scope of personnel that are trained through the Independent Study Program has grown by over 1000 percent. The increased number of trainees, FEMA's integration into DHS, and new training requirements post 9/11, required the redesign of the data collection tool used for the Independent Study Program; because the data collection tool needed to be redesigned, the system's privacy impact also needed to be reassessed.

Section 1.0
Information collected and maintained

The following questions are intended to define the scope of the information requested as well as the reasons for its collection as part of the system, rule, and/or technology being developed.

1.1 What information is to be collected?

The information is collected on a paper version of the new data collection form (FEMA Form 95-23). Once the new form is approved, an electronic version of the form will be available at the FEMA, EMI training web site for the Independent Study Program www.training.fema.gov/EMIweb/IS. The following information is to be collected:

- Last Name
- First Name
- Middle Initial
- Suffix
- Shipping Address
- City
- State
- Zip Code + Four
- Organization or Affiliation Category
- DHS Affiliation
- Other Federal Agencies
- Type of Organization or Affiliation

- Current Status (in the organization)
- Organization Name
- Organization Address
- City
- State
- Zip Code + Four
- Organization County/Parish
- Tribal Name (if applicable)
- Organizational Local Jurisdiction (if applicable)
- Date of Birth
- Social Security Number
- Work Phone
- Home Phone
- Course Code
- Email Address

1.2 From whom is information collected?

The information being collected for EMI's Independent Study Program comes from Federal, State, local and Tribal emergency management personnel and the general citizenry of the United States.

1.3 Why is the information being collected?

The purpose of ISDBS is to collect and maintain student training completion information. The information collected allows us to create and update student records, track completions and failures and issue completion certificates. This information is also used to issue college credit for completion of EMI IS courses, as well as issuing student transcripts to be provided to institutions for helping the student obtain continuing education units and/or to military institutions for military personnel to earn retirement points for successful completion of IS courses.

In addition, the ISDBS also maintains training completion data for the National Incident Management System (NIMS) training courses that are required of all Federal departments and agencies through Homeland Security Presidential Directive 5, "Management of Domestic Incidents". This individual student completion data is reported to the State Training Officers (STO) in order to ensure compliance with NIMS as defined by HSPD-5 and HSPD-8.

1.4 What specific legal authorities/arrangements/agreements define the collection of information?

The Independent Study (IS) Program is authorized under the Robert T. Stafford Disaster Relief and Emergency Act, Public Law 93-288 as amended and the ISDBS maintains the data to support this program. Homeland Security Presidential Directive 5, "Management of Domestic Incidents" directive also defines the collection of this information. In order to be able to provide training completion data to the State, local, and Tribal emergency management agencies to satisfy their compliance with HSPD-5 and HSPD-8, it is necessary to collect registration information as well as organizational data. This data is entered into a secure government database and all paper submissions are placed in locked storage areas in accordance with records management regulations. In the redesign of our database we are researching the ability to discontinue using the Social Security Number and using a unique identifier in its place.

1.5 Privacy Impact Analysis: Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated.

The privacy risks that have been identified include the collection of Privacy Act protected data such as Social Security Number (SSN) and home address. As this database is enhanced we will be moving away from using the SSN as the unique identifier in the system and instead using a unique identifier such as a randomly generated number. Currently, students can opt-out of providing their SSN, by requesting an assigned student number. We will not be able to discontinue collecting home address information, since some of our audience is the general public. Also, a privacy risk was identified in terms of collecting this data electronically. The electronic version of the form will be available at the FEMA, EMI training web site for the Independent Study Program www.training.fema.gov/EMIweb/IS will encrypt the data and send it to the server to be parsed into the Independent Study database to mitigate the privacy risk.

Section 2.0
Uses of the system and the information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

Similar to Section 1.3, this information is used to maintain student training completion information. The information collected allows us to create and update student records, track completions and failures and issue completion certificates. This information is also used to issue college credit for completion of EMI IS courses, as well as issuing student transcripts to be provided to institutions for assisting students in obtaining continuing education units and/or to military institutions for military personnel to earn retirement points for successful completion of IS courses.

In addition, the ISDBS also maintains training completion data for the National Incident Management System (NIMS) training courses that are required of all Federal departments and agencies through Homeland Security Presidential Directive 5, "Management of Domestic Incidents. This individual student completion data is reported to the State Training Officers (STO) in order to ensure compliance with NIMS as defined by HSPD-5 and HSPD-8.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern (Sometimes referred to as data mining)?

No analysis of this type is done within the system.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

Information for data such as what business area the student is representing is validated against a list of valid responses. For example, the system automatically verifies that the students' Last Name matches with the Social Security Number that is in the system when their exam submissions are received. If they do not match, the submission is not processed and the student is notified to contact the IS Office to resolve the issue. We are also designing and implementing a way for the IS staff to check a data table to correct names that have been inadvertently reversed and allow them to resubmit the exam submission. No other accuracy checks are done, as the information provided by the student is assumed to be accurate. Data is periodically reviewed to ensure that each student has a complete transcript record. In addition, the IS staff also corrects information on a daily basis and cleans up records based on student inquiries.

Audit trails are available within the system to track users that performed the data manipulation actions. Periodically, these trails are queried to ensure that the system is working as designed. If an individual was found to be using the information inappropriately, immediate disciplinary actions would be taken.

2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.

A weekly status report is given to the Contracting Officer's Technical Representative (COTR) to review how many forms were processed, certificates issued, college credit requests and transcript requests were processed. Periodic reviews of the processes and uses are done by the COTR. Student completion data provided to STOs indicate the need to safeguard information that is provided to them.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What is the retention period for the data in the system?

Deleted items are retained in archiving areas for a period of 90 days. Other data is retained indefinitely. Database records are backed up twice daily in a secured file server room. These files are backed up nightly to tape media. Backup tapes are stored in a separate area from the file server room for two weeks. A monthly tape backup is stored off-site in a secure environment and is retained for six months. Paper exam submissions are stored in secure file cabinets for 90 days from the date of receipt; then destroyed.

3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

No. It is in accordance with FEMA Manual 5400.2 Records Management Files Maintenance and Records Disposition. The information is retained for this period of time to ensure that if there is a system failure we could reboot and/or recreate the system as needed. Paper forms are kept for 90 days to allow us to pull the forms if there are student inquiries and/or to allow us to refer back to them in case a typographical mistake was made.

3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

As mentioned above in 3.1 and 3.2, the archived information is retained for 90 days to allow the system to be recreated if needed, as well as to restore a record that was inadvertently deleted. The paper forms are kept for 90 days to allow us to verify student information on the forms, as needed.

Section 4.0 Internal sharing and disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organizations is the information shared?

This information is shared via the Training Information Access System (TIAS) with the National Emergency Training Center Admissions System, FEMA Regional Training Managers, EMI Course Managers and limited to individuals with access to the FEMA intranet. Information may also be shared using Homeland Security Information Network (HSIN) and or DisasterHelp.gov.

4.2 For each organization, what information is shared and for what purpose?

Non-privacy Act data is displayed via TIAS, which includes, the student's name and organizational address, training courses completed and dates of completion. This is used as a way for EMI Course Managers and Regional Training Managers to verify Independent Study prerequisite courses have been completed prior to classroom training. This also allows FEMA staff to view their training completion transcripts. Information shared via HSIN or DisasterHelp.gov would allow easy access for other organizations within DHS to access their training completion information, since they do not have access to TIAS. These venues would also allow vetted users from States, such as State Training Officers, access to the information as well.

4.3 How is the information transmitted or disclosed?

Limited non-Privacy Act information is viewable through the TIAS web-application. You must be on a government computer with access to the FEMA intranet in order to access TIAS and this data. The ISDBS mailing information is no longer displayed in TIAS since this could have potentially been a home address which is protected by the Privacy Act. Only non-Privacy Act information would be provided via HSIN and DisasterHelp.gov.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

The main privacy risk identified was that the system is based on the SSN and contains other Privacy Act protected information which should not be disclosed. This was mitigated by only allowing non-Privacy Act information for users to view, such as Name, Organizational address, Course code, Course title, and Course completion date.

Section 5.0
External sharing and disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes Federal, state and local government, and the private sector.

5.1 With which external organizations is the information shared?

Specific state course completions are shared with each State Training Officers (STOs) from State Emergency Management Agencies. Also, specific training records are shared with other Federal Agencies, such as the Public Health Services, which obtain completions for just their employees. Information will also be shared to Office of Personnel Management (OPM) for the Enterprise Human Resource Integration (EHRI) government initiative. In addition, individuals will be able to specifically view their own training records through our web-reporting feature later this fiscal year.

5.2 What information is shared and for what purpose?

State training completion information is shared with each State Training Officer in order for them to prove NIMS compliance in order to receive Federal grant funding, as well as for them to track training completions for their state. The information that is shared includes individual data for students from their state and includes the following:

Completion Date, Last Name, First Name, Middle Initial, Suffix, Address Line 1, Address Line 2, City, State, Zip, Home Phone, Work E-Mail, Course Code, Course Title, Course Sub-title, and the Last Four of their SSN.

The information that is shared with Public Health Service is for them to verify NIMS course completion and compliance. The information shared is strictly on individuals from the Health and Human Services Agency and includes the following: SSN (which can be truncated to the last 4 digits), Email address, Last name, First Name, Middle Initial, Suffix, Phone number, Course Number, Course name, Completion Date, Pass/Fail Status, Score, Address Line 1, Address Line 2, City, State, and Zip code.

Information provided for EHRI is to comply with OMB and OPM reporting requirements for training data on Federal employees and including the following: Social Security Number, Course Title, Course Sub-title, and Course Completion Date. The web-reporting feature will allow students to access their own individual training data.

The individual will be able to view only their Course Completion Date, Last Name, First Name, Middle Initial, Suffix, Course Code, Course Title, and Course Sub-title for each course they have completed. The State Training Officer will be able to view the same information list above for individuals from their state. Logins and passwords will be required to access this data.

5.3 How is the information transmitted or disclosed?

A monthly report is provided which contains the data for the State Training Officers. The data is sent via CD-ROM. The CD-ROM is mailed with a signature confirmation and return receipt. A report for the Public Health Service is created every Tuesday and is hand-delivered on an encrypted flash drive. The information for EHRI will be sent via an XML file. It has not been determined exactly how this information will be transmitted as of yet. The web-reporting feature data will be displayed to the students and State Training Officers via a web-reporting page. Security protocols, in accordance with DHS standards will be taken to prohibit unauthorized personnel from accessing student information.

5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

No. Currently there is no written agreement in place. However, each CD-ROM that is provided to the State Training Officer contains a CD cover, as well as the letter accompanying the CD-ROM that indicates the need to safeguard the data and not disseminate it.

5.5 How is the shared information secured by the recipient?

State Training Officers take the appropriate steps to ensure the data is safeguarded and not disclosed to unauthorized personnel.

5.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

A one-hour audio conference will be held prior to receiving access to the information.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

The privacy risk identified was providing Privacy Act protected data in a secure fashion to individuals external to the organization. Mitigation efforts included limiting the information as much as possible, such as only providing a partial SSN and not the full SSN, as well as encrypting the data when possible and designing the web reporting feature to use a unique identifier and not the SSN.

Section 6.0
Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice. If notice was not provided, why not?

Yes. The data collection form contains a Privacy Act notice. In addition, the Privacy Act notice had been included on the form. Because the data collection forms are changing in order to collect more organizational type data, a new Federal Register Notice will be posted as part of the OMB Submission of the new data collection tool. A copy of Privacy Act notice is included as an appendix to this document.

6.2 Do individuals have an opportunity and/or right to decline to provide information?

Students can opt-out of providing their Social Security Number. In order to do this, they must provide some type of documentation of proof of U.S. citizenship (i.e. voter's registration card, birth certificate, and/or passport). After receiving this documentation a unique student number will be issued to them. Students' Last Name, First Name, Shipping Address, City, State, Zip Code, Course Code, E-mail Address (if submitting on-line) and Exam Answers will be required in order to process the submission and they will not be able to decline providing that information.

6.3 Do individuals have the right to consent to particular uses of the information, and if so, how does the individual exercise the right?

The individual does not have the right to consent to particular uses of the information. However, during the comment period after the Federal Register Notice is posted all individuals have the opportunity to inquire and comment on the uses of the information.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

No particular privacy risks were identified regarding the notice provided to the individuals above. Students can choose to request a unique student number in place of using their SSN and can use the address of their choice to receive their certificate.

Section 7.0 Individual Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures which allow individuals to gain access to their own information?

Currently students must call the Independent Study Office and request a transcript to see the courses that they have completed. Once the web reporting feature is implemented, certificate and transcript information will be available to them to view on-line.

7.2 What are the procedures for correcting erroneous information?

Students can call or send an email to the IS Program office to request the correction of erroneous information. In addition, IS staff throughout their daily operations and telephonic or e-mail interaction with students correct, consolidate and delete information as necessary and appropriate.

7.3 How are individuals notified of the procedures for correcting their information?

Procedures for correcting information are located on our EMI Contact Us webpage of our website (http://www.training.fema.gov/EMIWeb/contactus.asp). In addition, if the system finds potentially erroneous information, such as a Last Name and Social Security Number that does not match what is in our system, the student will receive an email notifying them to review the information provided and resubmit their exam if they had made a typographical error while inputting the information or to contact the IS Office to resolve the issue.

7.4 If no redress is provided, are alternatives available?

N/A

7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, explain the procedural rights that are provided and, if access, correction and redress rights are not provided please explain why not.

As mentioned in 7.3, procedures for correcting information are located on our EMI Contact Us webpage of our website. This website gives the students access to frequently asked questions and directs them to contact the IS Office directly if they have questions about the following items: IS Course Certificate, Student Transcript, Social Security Number, Password or login issues, Pass/Fail Confirmation, Update Personal Information, CEU Information, and Submitted wrong exam. In addition, if the student would like to have their information deleted from the system altogether, this can be done with a written request. This happens very infrequently and is handled on an individual basis.

Section 8.0
Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 Which user group(s) will have access to the system?

The following users have general access to the ISDBS; IS Contracting Officer's Technical Representative (COTR), Distance Learning program staff, IS Office contract staff, IT specialists, and IT programmers and database analyst contractor staff. The students will have limited access to only their individual records within the web reporting feature. State Training Officers will have limited access to only the records of individuals from their state.

8.2 Will contractors to DHS have access to the system? If so, please submit a copy of the contract describing their role to the Privacy Office with this PIA.

Yes. All the contractors are required to sign Non-Disclosure statements, provide information for background checks and must complete IT security training prior to accessing the database. The contractors enter the information into the database system and handle all the administrative support functions of the program, such as answering student phone calls and email inquiries, and printing certificates, failure letters and transcripts. A copy of the contract is provided as a separate document.

8.3 Does the system use "roles" to assign privileges to users of the system?

The system is separated into areas, such as demographics and courses. Users are provided access to these individual areas. Within the area, users have rights to add, edit and delete; there is no read-only access.

There are several other specific rights, such as deleting a student record, that are granted separately from the area rights.

8.4 What procedures are in place to determine which users may access the system and are they documented?

The IS COTR and/or the Distance Learning Section Chief determine whether users may have access to the system, based on their need and job position in support of the

Independent Study Program. A request is then sent to the IT specialists on campus to provide the access to the system. No specific procedures are documented.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

No specific procedures are documented. If an employee no longer works for the organization or no longer requires rights to specific functions, a HelpDesk ticket is issued by the COTR for the IS support contract advising the development support contractor to remove or restrict access as appropriate.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

None.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

Privacy is discussed at the time the Non-Disclosure statement is signed. The individual contractor is required to sign a similar non-disclosure statement for the company that they work for as well. Privacy will also be included in the Standard Operating Procedures of the Independent Study Program.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

This system is currently under the C&A of another system, the FEMA Employee Knowledge Center (FEKC). When the ISDBS was placed under the FEKC, IT Cyber Security indicated that minor systems and sub-systems did not require a full C&A.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

One privacy risk identified was providing overall rights to database for all users. This was mitigated by determining the need of the users and only allowing rights to specific areas of the database. Another privacy risk is to allow individual access to student personal data. This is necessary in order for the contractor to meet their contractual obligations in support of the IS Program. The non-disclosure statement used by both the contracted company and the government is important to mitigating the privacy risk because they are required to sign indicating that understand they are working with sensitive data and will not disclose it.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 Was the system built from the ground up or purchased and installed?

The system was built from the ground up and was designed to replace a legacy system. It used industry-best practices available at the time.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

The data resides on a server that is only accessible to FEMA-authorized users. Access is further protected through authentication for the application, using a login and password.

9.3 What design choices were made to enhance privacy?

In the redesign of our database, we are changing the unique identifier from the Social Security Number to enhance privacy. In addition, we eliminated unnecessary information in the display of student records on TIAS and are only providing limited information via the web reporting tool.

Conclusion

The Independent Study (IS) Program is authorized under the Robert T. Stafford Disaster Relief and Emergency Act, Public Law 93-288 as amended. Homeland Security Presidential Directive 5, "Management of Domestic Incidents" directive also defines the collection of this information. The Independent Study Database System (ISDBS) is the system that captures this data. Its purpose is to collect and maintain student training completion information and maintain training completion data for the National Incident Management System (NIMS) training courses that are required of all Federal departments and agencies, to be able to provide training completion data to the State, local, and Tribal emergency management agencies to satisfy their compliance with HSPD-5 and HSPD-8.

The data collection form contains a Privacy Act notice. In addition, the privacy policy had been posted in the Federal Register Notice.

The system was built from the ground up and was designed to replace a legacy system. It used industry-best practices available at the time.

Non-privacy Act data is shared via the Training Information Access System (TIAS) limited to individuals with access to the FEMA intranet. The web reporting feature will allow individuals limited access to their training completion information and State Training Officers limited access to training completion data for their state. This will require a login and password in order to obtain access and users will be vetted. Specific state course completions are currently shared with each State Training Officer each month by CD-ROM. Each State CD-ROM contains information stating that this information should not be disclosed.

Also, specific training records are shared with other Federal Agencies, such as the Public Health Services, which obtain completions for just their employees. Information will also be shared to OPM for the Enterprise Human Resource Integration (EHRI) government initiative.

Access to the Independent Study database itself is limited to the Independent Study (IS) Contracting Officer's Technical Representative (COTR), Distance Learning program staff, IS Office contract staff, IT specialists, and contracted IT programming staff.

All the contractors are required to sign Non-Disclosure statements, provide information for background checks and must complete IT security training. Federal staff is also required to complete IT security training.

Responsible Officials

<<Privacy Officer/Project Manager>>

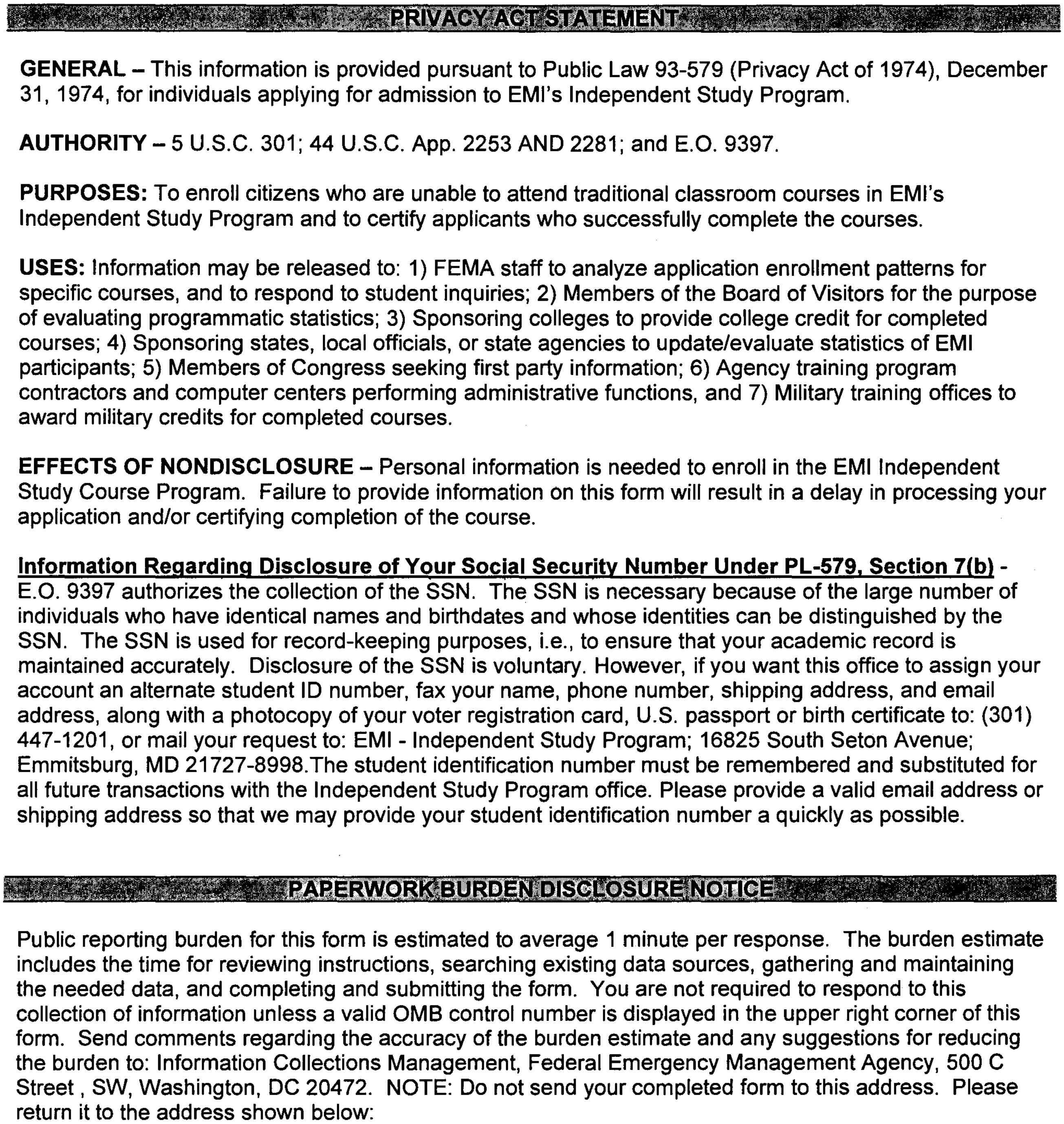
Department of Homeland Security

Approval Signature Page

________________________________ <<Sign Date>>

Maureen Cooney
Acting Chief Privacy Officer
Department of Homeland Security

Appendix A: Privacy Act Notice on 95-23 form.



PRIVACY ACT STATEMENT

GENERAL – This information is provided pursuant to Public Law 93-579 (Privacy Act of 1974), December 31, 1974, for individuals applying for admission to EMI's Independent Study Program.

AUTHORITY – 5 U.S.C. 301; 44 U.S.C. App. 2253 AND 2281; and E.O. 9397.

PURPOSES: To enroll citizens who are unable to attend traditional classroom courses in EMI's Independent Study Program and to certify applicants who successfully complete the courses.

USES: Information may be released to: 1) FEMA staff to analyze application enrollment patterns for specific courses, and to respond to student inquiries; 2) Members of the Board of Visitors for the purpose of evaluating programmatic statistics; 3) Sponsoring colleges to provide college credit for completed courses; 4) Sponsoring states, local officials, or state agencies to update/evaluate statistics of EMI participants; 5) Members of Congress seeking first party information; 6) Agency training program contractors and computer centers performing administrative functions, and 7) Military training offices to award military credits for completed courses.

EFFECTS OF NONDISCLOSURE – Personal information is needed to enroll in the EMI Independent Study Course Program. Failure to provide information on this form will result in a delay in processing your application and/or certifying completion of the course.

Information Regarding Disclosure of Your Social Security Number Under PL-579, Section 7(b) - E.O. 9397 authorizes the collection of the SSN. The SSN is necessary because of the large number of individuals who have identical names and birthdates and whose identities can be distinguished by the SSN. The SSN is used for record-keeping purposes, i.e., to ensure that your academic record is maintained accurately. Disclosure of the SSN is voluntary. However, if you want this office to assign your account an alternate student ID number, fax your name, phone number, shipping address, and email address, along with a photocopy of your voter registration card, U.S. passport or birth certificate to: (301) 447-1201, or mail your request to: EMI - Independent Study Program; 16825 South Seton Avenue; Emmitsburg, MD 21727-8998.The student identification number must be remembered and substituted for all future transactions with the Independent Study Program office. Please provide a valid email address or shipping address so that we may provide your student identification number a quickly as possible.

PAPERWORK BURDEN DISCLOSURE NOTICE

Public reporting burden for this form is estimated to average 1 minute per response. The burden estimate includes the time for reviewing instructions, searching existing data sources, gathering and maintaining the needed data, and completing and submitting the form. You are not required to respond to this collection of information unless a valid OMB control number is displayed in the upper right corner of this form. Send comments regarding the accuracy of the burden estimate and any suggestions for reducing the burden to: Information Collections Management, Federal Emergency Management Agency, 500 C Street , SW, Washington, DC 20472. NOTE: Do not send your completed form to this address. Please return it to the address shown below:

ENROLLMENT OPTIONS:

MAIL:
Federal Emergency Management Agency
EMI-Independent Study Program
16825 South Seton Avenue
Emmitsburg, MD 21727-8998

FAX: (301) 447-1201

INTERNET:
http://training.fema.gov/EMIWeb/

EQUAL OPPORTUNITY STATEMENT

The Emergency Management Institute (EMI) and the national Fire Academy (NFA) are equal opportunity institutions. They do not discriminate on the bases of age, sex, race, color, religious belief, national origin, or disability in their admissions and student-related procedures. In addition, employment related decisions based on sexual orientation are prohibited. Both schools make every effort to ensure equitable representation of minorities and women in their student bodies. Qualified minorities and women are encouraged to apply for all courses.