Privacy Impact Assessment
for the

Application and Registration Records for Training and Exercise Programs

September 22, 2009

Contact Point
Tammi Hines
Privacy Branch
Federal Emergency Management Agency
202-646-3606

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0347

Abstract

Many of the Department of Homeland Security Federal Emergency Management Agency (FEMA) training and exercise programs collect a minimum amount of information. The information collected and maintained is for the purpose of, but not limited to, providing training to individuals, fund reimbursements related to training and exercises, training coordination, and other training related objectives. Still other systems provide, but are not limited to user development, evaluation, and improvement planning tools, which together provide Federal, State, local emergency response planners the timelines, templates, example documentation, and policy guidance needed to effectively manage and execute their exercise and training projects. This Privacy Impact Assessment (PIA) documents the collection and safeguarding of personal identifiable information by FEMA in support of its training and exercise programs. The courses and programs made available through the various training and exercise programs provided for by FEMA and/or its program directorates enables individuals from local, tribal, state, federal agencies as well as the public in many cases to take various types of locally facilitated and distance learning courses on an electronic platform. Meanwhile, there are other programs, which have systems created with security and preparedness distinctly in mind, which align purpose and mission by facilitating training and exercises to allow for improved practices, response planning, innovation, and overall preparedness for the Nations Homeland Security and emergency response professionals.

Overview

FEMA has several program and IT systems throughout its directorates and field offices that manage FEMA’s various training and exercise programs. These programs provide training and situation exercises to Federal emergency response and emergency management personnel, as well as International, Intrastate (multi-county), State, Local, Tribal, Regional (multi-state), Nongovernmental/Volunteer Organizations, and Private Sector personnel. The various IT systems and programs educate and empower FEMA and the aforementioned personnel to support FEMA’s mission to reduce the loss of life and property. Also the use of the systems will aide in the protection of the Nation from all hazards, including natural disasters, acts of terrorism, fires and other man-made disasters, by leading and supporting the Nation in a risk-based, comprehensive emergency management system prevention, preparedness, protection, response, recovery, and mitigation.

The various training and exercise programs include information for the purpose of, but not limited to, student application for training/participation reimbursement for expenses, program evaluation (Federal, State, and local programs), coordination of training, training and exercise development, and student/participants evaluations. Information maintained in the system may be shared with other federal, state, local and private/public organizations for the purpose of training and exercise development; tracking of participation in training and exercise programs; coordination of training and exercises; and for statistical purposes to determine the preparedness level of the nation.

This PIA intends to cover all of FEMA's Training and Exercise Program systems. The following two systems are just two representations included but are not limited to the many training and exercise programs and IT systems owned and managed by FEMA; thus covered by this PIA:

Exercise System:

- **National Exercise Master Scenario Event List (NxMSEL)**

Training System:

- **FEMA National Shelter System w/National Shelter System Computer Based Training (NSS-NSS CBT)**

The following is a description of each of the representative training and exercise systems/programs:

National Exercise Master Scenario Event List (NxMSEL)

The Department of Homeland Security (DHS) Federal Emergency Management Agency (FEMA National Preparedness Directorate (NPD operates the (NxMSEL). NxMSEL is an automated system specifically designed to assist in Master Scenario Event List (MSEL) management. A MSEL is a chronological timeline of expected actions and scripted events (i.e., injects) to be inserted into operations-based exercise play by controllers in order to generate or prompt player activity and ensure completion of exercise objectives. During exercise execution, NxMSEL provides tools for tracking progress and for reviewing, modifying, and releasing injects to the training audience. The NxMSEL design exists to support geographically dispersed organizations and a wide variety of functional areas in a collaborative, data-sharing environment and it supports both subject matter expert (SME) users and MSEL Managers. The system also supports lessons learned development and data gathering during post exercise operations.

NxMSEL may provide access to Sensitive But Unclassified (SBU) information and therefore, access is limited to approved exercise participants from federal, state, territorial, and local governments, as well as private-sector organizations and non-governmental organizations. Access to system data is role-based, meaning that users only have access to exercises to which the system assigns the user a formal role.

National Shelter System w/National Shelter System Computer Based Training (NSS-NSS CBT)

FEMA is named as the primary agency responsible for mass care service and emergency assistance in Emergency Support Function # 6 (ESF #6) of the National Response Plan (NRP). The National Shelter System (NSS) National Shelter System Computer Based Training (NSS CBT) which is under the authority of the Individual Assistance Division and Disaster Assistance Directorate, MASS Care ESF #6. FEMA and the ESF #6 supporting agency, the American Red Cross (ARC), developed the NSS. NSS-NSS CBT is a coordinated data system containing information for thousands of emergency shelter resources nationwide with front-end functionality (NSS CBT) of web-based training for new users of the National Shelter System. Emergency Management at all levels can use the NSS to identify, track, analyze, and report on shelter preparedness and operations data in a consistent and reliable manner. The NSS will provide Federal, State, and Local emergency management professionals in both the public and private sectors the capability to manage and report upon emergency shelter related information. NSS has the capability to store, retrieve, update, and report on shelter information including management, population, and incident information. The NSS has the ability to track virtually any type of shelter or facility used in response to disasters. In addition to traditional Shelters, examples include:

- Pet shelters, Kitchens
- Points of Distribution (POD’s), Warehouses
- Warming cooling and Respite centers
- Embarkation, Debarkation, and Reception processing sites
- Any site related to the management of the people affected by the operation

The NSS also includes an enhanced Geographic Information System (GIS) mapping function that will allow emergency management professionals to see in real time, shelter locations, critical infrastructure, flood plains, fault lines, and numerous other geospatial elements.

Additionally, FEMA is working to insure the system is interoperable with the Red Cross NSS, Web-EOC, and several other Emergency management programs allowing them to share data, eliminating the need to enter data in multiple applications.

The front-end functionality (NSS CBT) will be a web-based training for new users of the NSS. The NSS CBT will reside on FEMA.gov. _The training will launch using a flash file. _The trainings design is for federal, state, local, tribal governments, volunteer organizations, and non-profit organizations working with shelter operations during emergencies. _This training (or the in-class equivalent) is required for users who need access to the NSS.

This training contains the following content:

- Module 1: “Overview of the FEMA NSS”
- Module 2: “NSS Training for User Levels 1-4”
- Optional Module: “What’s New in the FEMA NSS”

After users read the content, they must pass a 15, 35, or 50-question test, after which time, they will receive a certificate of completion and NSS will receive a submission for access pertaining to the user. Users who choose to take the test at the end of the training will fill out the following information, and then the Mass Care team at FEMA HQ will receive the information via email. No personal information will be stored in the program. An email of the information transmittable from and to a DHS email account through FEMA’s secure network.

- Users First Name (e.g. Fred)
- Users Last Name (e.g. Anderson)
- Users email address (e.g. fred.anderson@dhs.gov)
- Users telephone number (e.g. 555-555-5555)
- Organization affiliation (e.g. FEMA)
- Organization City (e.g. Washington)
- Organization State (e.g. DC)
- Organization Phone Number (e.g. 555-555-5555)
- POC at the Organization (e.g. Supervisor Martin)

The system will generate an email using a DHS email account with the users name and the organizations’ information which, will be sent to the Mass Care Branch DHS email account at FEMA HQ, therefore it will connect with FEMA’s secure email exchange server.

The Mass Care Unit within the Individual Assistance Division and Disaster Assistance Directorate is the owner of the system.

Various legal authorities govern FEMA’s training and exercise programs. However, the underpinning legal authority is the Robert T. Stafford Disaster Relief and Emergency Act.

Section 1.0 Characterization of the Information

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

1.1 What information is collected, used, disseminated, or maintained in the system?

The following is a listing which details a compilation of required/not required fields of information that systems collect as part of the user registration process, however not all systems collect this complete list of data. Many systems will collect the following information via email only in a web-form from and to a DHS email account through FEMA's secure network. The list of information collected is not limited to but may include (required information is marked with an "*") List includes fields from the NSS-NSS CBT training and NxMSEL exercise systems as well as other systems comprising this document:

Training systems have uses that develop and provide training courses, which inform individuals of their roles and responsibilities within a particular system or response plan and teach skills related to those roles and responsibilities, thereby preparing them for participation in exercises, tests, and actual emergencies related to response plans. Although training systems gather the same types of information that are collected by an exercise system, these systems gather additional information which is required for course registration, tuition payments and tuition reimbursements. The following list details the additional information collected by training systems:

NSS-NSS CBT Training System

- Users First Name (e.g. Fred)
- Users Last Name (e.g. Anderson)
- Users email address (e.g. fred.anderson@dhs.gov)
- Users telephone number (e.g. 555-555-5555)
- Organization affiliation (e.g. FEMA)
- Organization City (e.g. Washington)

- Organization State (e.g. DC)
- Organization Phone Number (e.g. 555-555-5555)
- Point of Contact (POC) at the Organization (e.g. Supervisor Martin)

No Personal Information will be stored in NSS CBT. The email will be stored on FEMA's secure Exchange Server.

Exercise systems provide a workspace for users to schedule, plan, and perform simulated responses to a variety of possible real world incidents and emergencies to validate the viability of one or more aspects of an emergency response plan. The functionality and classification of an exercise system determines the depth of information requested from the user during the registration process.

NxMSEL Exercise System:

- Rank*
- First Name*
- Last Name*
- Service*
- Position
- Command/Organization
- Command/Organization Phone Number*
- Email Address – Unclassified*
- Email Address – Classified
- Exercise Name*
- Cell phone*
- Reason for requesting access

Compilation of other training and exercise systems information collection fields:

- First Name,
- Middle Name,
- Last Name*,
- Date of Birth,

- Sex,
- Ethnicity and Race,
- U.S. Citizenship (city and country of birth is also included for non-citizens)*,
- Social Security Number (SSN) or an alternate number that has been assigned in lieu of the SSN which is provided voluntarily and will be discontinued after FEMA identifies a new unique identifier format, (only a limited number of systems request this information)
- Home address (including Street, City, State, and Zip code + Four),
- Home phone number,
- Command/Organization (e.g. state, military, local/federal Government users)
- Professional/Organization phone number*,
- Point of Contact (POC) at the Organization (e.g. Supervisor Martin)
- Alternate phone number*,
- Cell phone,
- Job Title*,
- Professional Address, including Street, City, State, Zip code, and Country*,
- Time Zone,
- Professional Email Address/ Classified Email Address,
- Alternate Email Address/ Unclassified Email Address*,
- Professional Fax number,
- Rank/ Prefix* (if applicable),
- Service* (if applicable),
- Position*,
- Exercise/Training name*,
- Exercise/Training type*,
- Exercise conduct dates,

- Exercise mission,
- Exercise target capabilities,
- Reason for requesting access,
- Primary responsibility and type of experience or discipline,
- Number of years of experience,
- Scenario details,
- Venue,
- Controller,
- Player,
- DHS Affiliation (the component in DHS),
- Other Federal Agencies (i.e. USDA, DOD, etc.),
- Organization affiliation,
- Organization name,
- Organization phone number,
- Organizational type (Federal, International, Intrastate (multi-county), local, nongovernmental/volunteer organization, private sector, regional (multi-state) state and tribal),
- Current status in the organization (Paid Full-time, Volunteer, etc.),
- Organization address, including City, State, and Zip code + Four,
- Organization Country/ Parish,
- Organization Local jurisdiction (if applicable),
- Point of Contact (POC) at the organization,
- Number of staff in organization,
- Size of population served by the organization,
- Tribal Name (if applicable),
- Fire department identification number*(if applicable),
- Current position and years in that position,
- Category of the position,

- Employment verification, including First and Last Name, Email Address, Phone Number, Job Title, and Relationship to Reference of Point of Contact (POC)* (if applicable),
- Employment status,
- Password (Certain applications all users to select his/her own password during the initial user registration/application process. When done the information is stored within an encrypted database).
- Course pre-requisites as described in the course catalog,
- Course code,
- Course title,
- Course location,
- Course dates requested,
- Indication if special assistance for a disability is required (requested if housing is to be provide at the resident facility),
- Exam answers,
- Security questions (2) – (Varies per application/system and may or may not be required for resetting password created if user forgets password) e.g. what city were you born in, what is the name of your favorite sports team, and what model was your first car?

Users provide personal information on a voluntary basis. Failure to provide certain information requested of the registrant may result in a delay in processing an application because the identity and/or need for system use of the individual may not be fully verifiable. The Exercise and Training Programs have limited controlled use of information such as age, sex, and ancestral heritage, which uses the information for statistical purposes only.

The SSN may be necessary for some of the training and exercise systems due to the large number of individuals who may have identical names and birth dates and whose identities are distinguishable by their SSN. Disclosure of an individual's SSN is voluntary. However, if an applicant does not provide a SSN, a unique identification number is substituted, which may affect the ability of limited systems, which use an SSN to retrieve, complete training information on an applicant.

1.2 What are the sources of the information in the system?

FEMA's Training and Exercise Program receives information from members of the first responder, federal, state, local, tribal emergency management, and homeland security community's at all organizational and jurisdictional levels in connection with the account registration process. These communities include but are not limited to individuals that are not DHS/FEMA employees, such as local and state police, firefighters, Red Cross, and other emergency responders.

1.3 Why is the information being collected, used, disseminated, or maintained?

FEMA Training and Exercise Program collect information to provide a collaborative working environment for exercise program development and project management. For example, improvement plans and corrective actions are sharable among emergency responders such as state and local police, to assist in the prevention, preparation, and response to acts of terrorism and other incidents across disciplines and communities throughout the US.

FEMA collects information to create and update student records, track completions, failures, and issue completion certificates. These trainings and exercise program courses provide a consistent nationwide template to enable all government, private sector, and nongovernmental organizations to work together during domestic incidents. Including, but not limited to all training and exercise systems, organizations are required to meet compliance in order to receive grant funding from FEMA. Reports of individual student completion data is sharable with respective State Training Officers (STO), so that they can ensure compliance with directives set by the system.

1.4 How is the information collected?

FEMA's Training and Exercise Program may include, but is not limited to the collection of information by paper application, telephone, emails, or through secure web-based form, e.g., FEMA 75-5A, General Admissions Application Short Form authorized under OMB Report Control Number 1670-0002. The systems also utilize Secure Socket Layer (SSL) 128-bit encryption to protect applicant information.

1.5 How will the information be checked for accuracy?

In many cases, checking that information is accurate may include but is not limited to Support Services Administrators utilize the User Management area of the system to approve or deny applicants, update users' profile information, and reset passwords. These administrators confirm the applicant's information (identity and status as a first responder or Homeland Security official) by contacting a DHS or other government reference provided during the registration process. Some systems approval process include the receipt of email request for an account by a prospective applicant, a FEMA Regional POC must approve the applicantion. The Regional POC approval signifies the client information is correct and that the applicant has a valid reason to access the system.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

Collected information is pursuant to Homeland Security Presidential Directive 8 "National Preparedness" (HSPD-8) which establishes policies to strengthen the preparedness of the United States and allows for Federal preparedness assistance to State and local governments. The Homeland Security Presidential Directive 5 “Management of Domestic Incidents” (HSPD-5) enhances the ability of the United States to manage domestic incidents. The Homeland Security Act of 2002, Privacy Act of 1974 (5 U.S.C. 552a), E.O. 13111, Using Technology to Improve Training Technologies for Federal Government Employees and the E-Government Act of 2002.

To include, but not limited to the some applicable systems, training is a provision under PL 93-498, Federal Fire Prevention, and Control Act of 1974. Other authorities related to the collection of information in relation to providing the training include:

- Publication L, 93-579, 44U.S.C. 3101, Privacy Act of 1974 which relates to the protection of certain information and the requirement to include a statement in the application forms
- E.O. 12127, E.O. 12148; and the Reorganization Plan No.3 of 1978, 5U.S.C. 301relate to the creation of the FEMA

1.7 <u>Privacy Impact Analysis</u>: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

The privacy risks for the Training and Exercise Program include:

- Unauthorized Access/Disclosure
- Identify theft
- Social Engineering techniques
- Loss of data
- Inadvertent release of data

Privacy risks are identifiable based on the unauthorized theft or disclosure of the information outlined in this document. Individuals employing social engineering techniques (e.g., pretext calling, phishing, etc.) could potentially use this information to locate individuals, identify individuals in sensitive positions, and masquerade as an individual to gain access to sensitive systems.

With Personally Identifiable Information (PII) collected and transmitted across the internet in the clear, the possibility of interception exists, including the use of information in a harmful way. Some systems mitigate this risk by selecting approved hosting locations such as the Office of Personnel Management (OPM) GoLearn approved hosting locations.

To mitigate the risks associated with collecting PII, the program has integrated robust security into its risk management plans and through the Certification and Accreditation processes, which routinely tests the security of the system. By enforcing system policies, settings, and strong passwords, the program protects the privacy of data to promote or permit a secure environment for public access into and release of information to FEMA in the system. The security risk management measures also protect the integrity of the data itself. The Program has also implemented auditing to defend against misuse of the data and to monitor those with access to the information.

To minimize risks associated with access to the data, only contractors and Federal employees with a verified need to know have access to the Program. All contractors must meet the requirements for suitability and pass a background investigation in accordance with the DHS Sensitive Systems Handbook. Contractors must sign the appropriate non-disclosure agreements and agree to handle the information in accordance with the Privacy Act of 1974, as amended.

For systems that are outsourced to a third party contractor for use, the contractor personnel provide Support Services (Help Desk) support including user administration.

Section 2.0 Uses of 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.

The following may include, but is not limited to all systems uses of information. Information uses include enrolling applicants into courses, providing for completion certificates, maintaining transcripts, and communicating with selected students. Course exam statistics and/or course completions are reportable to a Training Specialist/Instructional System Specialist depending on mandatory training and other competency requirements. When done, reporting of course completions is reportable in accordance with Government Performance and Results Act requirements. Aggregate information is collectable by some but is not limited to all systems for reviewing and identifying patterns and trends to determine training effectiveness. Including but not limited to all systems, information provided by the applicant during the member registration is usable to confirm the individual’s identity, establish eligibility for system access, and provide and monitor system security. Additionally, the user selected “security questions” and a related answer associated with some systems is for the purpose of verification of a user’s identity over the phone when a user calls Support Services for assistance such as to reset a forgotten password.

The Exercise and Training Programs may use information in the following ways:

- Exercise and Training Programs may share improvement plans and corrective actions among emergency responders to assist in the prevention, preparation, and response to acts of terrorism and other incidents across disciplines and communities throughout the US. Some systems, in accordance with National Incident Management Systems (NIMS) may share information pertaining to training courses aligned with the requirements established under Homeland Security Presidential Directive 5, HSPD-5, “Management of Domestic Incidents”.
    - Some systems may report individual student completion data to customers, such as the State Officers (STO) in order to ensure compliance with NIMS as defined by HSPD-5 and HSPD-8.

- Some systems use web based project management tools and comprehensive tutorials for the design, development, conduction, and evaluation of exercises that help authorized systems users, which consist of Federal, State, and local emergency response and homeland security officials, resolve preparedness gaps or deficiencies in a systematic manner, strengthening national preparedness.
- (Varying by system), Once the user has obtained authorization, exercise POCs, lead planners, and participants may view other user names and email addresses assigned to an exercise or training. _

2.2 What types of tools are used to analyze data and what type of data may be produced?

The Training and Exercise Program does not utilize data mining to assist users in identifying previously unknown areas of note, concern, or pattern. The Program includes reporting and analysis tools to generate custom charts and graphs on Improvement Plans from preparedness exercises and real-world incidents. It also provides users with a number of pre-defined reports.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

The Training and Exercise Program does not use commercial or publicly available data in connection with the PII it collects and stores. In order to access information within the Training and Exercise Program, users and administrators must authenticate to the system. Information maintained for the purpose of the system is not publicly available.

2.4 <u>Privacy Impact Analysis</u>: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

To ensure that information handling occurs with the described uses above, the Training and Exercise Program when applicable has developed the program so that it requires a valid username and password to access the system. The form field for the password is masked. It uses industry-standard SSL-encryption to protect data transmissions. Only authorized users of the program may gain access to the information. It is mandatory for individuals who maintain access to take Security Awareness Training annually, and acknowledge and sign the rules of behavior for using FEMA information technology systems. To ensure accountability auditing is preformed and all user activities undergo logging procedures.

Support Services and server administrative personnel under go vetting in accordance with DHS SSH 4300A policy, and have received a favorably adjudicated Background Investigation (BI) as defined in DHS MD11055, Suitability Screening Requirements for Contractor Employees. PII contained within the Program receives handling under the same level of sensitivity and criticality as the Sensitive but Unclassified (SBU) information.

Section 3.0 Retention

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

3.1 What information is retained?

All information provided by the Exercise and Training Program applicants as outlined in section 1.1 and 1.3 of this PIA is retained in each of the applicants file (paper and or electronic).

3.2 How long is information retained?

User specific information, including PII collection, during the registration process is in keeping with the applicable NARA regulations. In some cases, this can be as little as five years and as long as 40 years. Training and exercise programs must refer DHS records retention schedule for their activity.

Information pertaining to training and training requests will no longer be available, destruction occurs five years after completion of the program.

3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

Yes. Each activity's retention schedule must receive approval by NARA (NARA Authority N1-311-88-2 1A, N1-311-08-2, and GRS series). They are published in FEMA Manual 5400-2M.

3.4 <u>Privacy Impact Analysis</u>: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

The risks associated with the length of time data is retainable including but not limited to:

- unauthorized access,
- PII could be maintained for a period long then necessary,
- Identity theft,
- Loss of data,
- Inadvertent release of data,

Although there is always risk inherent in retaining personal data for any length of time, the data retention periods identified in the NARA schedule are consistent with the concept of retaining data only for as long as necessary to support the agency's mission. To minimize risks, the program limits access to the data available, including when and how access handling occurs.

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 organization(s) is the information shared, what information is shared and for what purpose?

Training and Exercise information is sharable with internal DHS components if there is a "need to know" as stated in the routine uses section of the SORN and in compliance with the Privacy Act. The purpose of sharing the information internally is to validate a user's identity so that they may gain access to a training or exercise system. You may refer to section 1.1 to see the information shared.

4.2 How is the information transmitted or disclosed?

Information transmitted via telephone, paper or the use of a secure web portal, which utilizes SSL 128- bit encryption to protect user and system information will be the method used.

4.3 <u>Privacy Impact Analysis</u>: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

The risks associated with the sharing of information internally include but not limited to:

- Unauthorized access
- Personal acting in malicious an irresponsible fashion

- Loss of Data

The following mitigation steps were set in place but not limited to:

- Conducting audit trails and system logs which record each action by the user
- Provide password – protected and industry standard SSL –128 bit encryption used to protect data transmission.
- Make sure that only those who have a need to know are able to access the information.
- Make sure that contractors and employees receive the appropriate security awareness training.

Section 5.0 External Sharing and Disclosure

The following questions is 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 organization(s) is the information shared, what information is shared, and for what purpose?

The following information may not be sharable with external agencies other than as outlined in the "Routine Uses" in the SORN and listed under the Privacy Act Statement. The information within the Training and Exercise Programs is sensitive but unclassified, (this statement infers some but may not include all systems); therefore, access to the system is restricted to emergency response providers and Homeland Security officials. Information collected during the user registration process is sharable with any external organization that is involved in the process of validating the applicant's identity and need for system access. External organizations will vary depending on the organization listed by the user as a point of contact. Examples are below:

- Federal Agencies, Offices, Departments - unique identifier, course title and course completion date
- Sponsoring State or local officials and agencies (including State Training Officers) - student name, address, unique identifier, email address, course code, course title, and completion date to update and evaluate statistics of EMI participants.
- Emergency response providers

- Members of the Board of Visitors - number of course completions based on course code and state for the specific purpose of evaluating programmatic statistics.
- Sponsoring Colleges - student name, address, course code, course title, and completion date to provide college credit for completed courses.
- Member of Congress - student name, address, email address, course code, course title, completions date, or course completions based on course code and state for first party information requests.
- Agency training program contractors and computer centers - student name, address, organizational information, unique identifier, email address, course code, course title, completion date, score and answers to perform administrative functions of entering data into the system and responding to student inquiries.
- Military personnel or training offices - student names, addresses, course codes, course titles, completion dates and continuing education units to award military credit for completed courses.

Information in the program is sensitive but unclassified; therefore, access to the system is restricted. Information collected during the user registration process is sharable with any external organization that is involved in the process of validating the applicant’s identity and need for system access.

Information shared within the U.S. Treasury Department, Office of Personnel Management (OPM) for the Enterprise Human Resource Integration (EHRI) government initiative. EHRI is one of the 24 e-Government initiatives designed to support the President's Management Agenda (PMA). OPM's EHRI will support human resources management across the Federal Government at all levels from front-line employee to senior management. When fully implemented, EHRI will replace the current Official Personnel Folder (OPF) with an electronic employee record for all Executive Branch employees, resulting in a comprehensive electronic personnel data repository covering the entire life cycle of Federal employment, which includes employee training.

Training Records shared with EHRI would only include records from federal employees. Information provided for EHRI includes information on Federal employees only and includes the following information; unique identifier, course title and course completion date and is provided to comply with OMB and OPM reporting requirements for training data on Federal employees.

Information on individuals, e.g., organizational information may be sharable with national, state, and local fire and emergency management organizations upon request on as applicable by the training or exercise program administered.

Organizational information is available from the system on certain reports. The reports do not contain any personally identifiable information (PII) such as the names of individual students, with the exception of the roster report.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

Yes, if in accordance with General Information Technology Access Account Records System (GITAARS) DHS/ALL-004, May 15, 2008, 73 FR 28139 System of Record Notice (SORN). This PIA serves as notice regarding how DHS will use PII that may be collected and used by the Training and Exercise Programs. Additionally, when logging into the systems, users are notified that they are accessing a government system, that all access is subject to monitoring, and that there is no expectation of privacy in the course of the use of the system.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Information sharing occurs by:

- Telephone
- Electronic (use of a secure website)
- Paper means.

For information transmitted electronically, proper security measures taken, including SSL 128-bit encryption when necessary. For example, information may be transmittable via an authenticated web interface, and regulated via a role base under access controls. Information access is limited to the minimum necessary to perform required job functions.

When information is transmittable by paper means, FEMA will include a letter to the external agency indicating that FEMA’s Privacy Act records provide and indicate that they under the utilization for applicable routine use and that further disclosure of the records is not permissible.

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

The risks associated with external sharing may include but are not limited to improper handling of information and disclosure to unauthorized individuals.

Access to the system is limited to individuals authorized and validated by administrators. As a condition of system use, each authorized user is required to read and accept the system Rules of Behavior.

Each program/system may vary in their protection and mitigation methods, however generally, Admissions system owners, and administrators, both Federal and contractor employees are not to transmit or release any non-secure transmission of PII to an external entity. With PII collected and transmitted across the internet for purposes of the training and exercises by some systems, which utilize secure transmission methods, the possibility of interception is limited. Student SSN, DOB, Race, and Gender data that collected is generally encrypted utilizing 256-bit Advanced Encryption Standard (AES) technology and stored in completely different data set tables. Any data sharing will be limited to aggregate course completion data by course name and federal/state/local jurisdiction. As a condition of system use, each authorized user is required to read and accept the System Rules of Behavior. Audit trails and system logs are additional methods utilized by some systems to record each action performed by the users in the system. Periodically, these logs are under revision to ensure that users with administrative privileges act in a way that is consistent with the Rules of Behavior.

In addition, in accordance with the DHS Sensitive System Handbook, Training and Exercise Programs ensure affective security controls and authentication. By enforcing system policies, Rules of Behavior, system and application settings, and strong passwords, the programs mitigate risks of disclosure of PII when shares.

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?

Yes, Notice occurs in the following ways, but is not limited to:

A Privacy Act notice is included on the FEMA Form 75-5, General Admissions Application; 75-5a, General Admissions Application Short-Form; 75-3, Student Stipend Agreement; 75-3a, Student Stipend Agreement (Amendment) and the electronic versions of those forms. Notice provides the individual prior notice to the collection of information. Please visit www.fema.gov for further information regarding these forms.

PII is collected as part of the user registration process. Varying PIAs and SORNs including for example, the DHS Department-Wide system of records notice (SORN) General Information Technology Access Account Records System (GITARRS) serves as notice regarding how DHS will use PII that may be part of the collection and used by a program or system. Additionally, when logging into a system, users' notification appears to indicate that they are accessing a government system, and additionally that all access is subject to monitoring, and that there is no expectation of privacy in the course of using said system.

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

Yes, individuals have the option, opportunity, and/or right to decline to provide information. However, individuals declining to provide information that are system specific requirements for registration purposes, will receive a denial to access notification, whereas the systems' ability in varying systems to effectively manage and execute their projects through the timelines, templates, example documentation, policy guidance and other design, development, evaluation and improvement planning tools available from the prospective systems.

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

Generally, yes, unless the information is required for a specific purpose for which no other uses are appropriate. For example, the individual has the right to consent to particular uses of the information consistent with the routine uses ion the SORN and the Privacy Act Statement. However, in some cases, such as registering for exercises and training, the sole use of information is Compliance requirements set by the DHS Sensitive Systems Handbook and FISMA to verify applicants or users' identity or establish eligibility. In these circumstances no other uses for their information is appropriate.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Notice is under the provision of the individuals PII both in hard copy and the online Privacy Act Statement as a link to the privacy policy and is on the instructions for the actual forms. In addition, routine uses are included in the system of records notice.

Section 7.0 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 that allow individuals to gain access to their information?

Users are capable of accessing their information by calling their prospective Support Services Center that falls under the establishment for the training or exercise system they use. All users must enter authentication information (user ID/Password) to gain access to the systems. Further validation requires individuals to answer a security question. Individual users will only be able to access their own personal information. The affiliate organizations providing the systems for training and exercises are within compliance with all DHS e-Authentication requirements.

A web-based application will allow individuals to electronically access and view the courses only they have completed. If users are unable to access their records electronically, they may follow procedures outlined in FEMA and the DHS Privacy Act regulations, 44 CFR Part 6 and 6 CFR Part 5. Request for Privacy Act information must be in writing, and clearly marked as a “Privacy Act Request.” The name of the requester, the nature of the record sought, and the required verification of identify must be clearly indicated. Requests should be sent to; FOIA Officer, Records of Management, Federal Emergency Management Agency, Department of Homeland Security, 500 C Street, SW, Washington DC 20472.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Users may call, or send email to their Support Services Center that available for their training or exercise systems. Once the Support Services technician verifies the user’s identity, the user may then request the Support Services technician or senior technician to update their account information to reflect accuracy.

Certain organizational information on rosters is available during class attendance for verification and protection.

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

Individuals receive notification if certain eligibility information for a course is not given.

- Users receive notification of the procedures for correcting their information training and exercises through training on system features and use, from the online help guide and from their exercise managers.
- Users are given instructions onscreen through embedded help (and e-mail hyperlinks) within their training systems.

The ease of access to verify information and the capability of the user in correcting their information fully addresses the redress issue. Therefore, no redress alternatives are necessary..

7.4 If no formal redress is provided, what alternatives are available to the individual?

The systems generally collect personal information, at a limit, which is a collection of personal information by the individual during registration. Each time an individual submits an application for a course, the databases collect and an update occurs using the most recent information the databases receive. Individuals may provide updated information any time they would like. The Information in the database is only applicable to the course for which the individual applies.

Users may always contact the respective Support Services Helpdesk for assistance in redressing whatever issues they may encounter.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

The risks associated with the redress could include, but is not limited to misuse of data, loss of data, inadvertent release of data, and identity theft.

Risks are minimal by limiting accessibility to data by minimizing when and how access is given.

During enrollment activity, Students could inadvertently insert incorrect, inconsistent, and/or incomplete information. In many of the training and exercise systems, to allow for mitigation, users enter authentication information (user ID/Password) to gain access to the system. Individual users will only then be able to access and change their own personal information if necessary. Several of the systems alternatively have the option of requesting a correction by calling their prospective Support Services Centers.

Systems access, to and correction of information is also a provision many systems use through a web-based application as well as procedures outlined in the DHS Privacy Act Regulations, 44 CFR Part 6 and 6 CFR Part 5.

In most instances, the individual applicants provide their own information. There is no need to update it unless the applicant has put in an application for subsequent class(s) and provides an update to their information. An individual who has applied for a course can provide an update any time to their information, and their record will reflect the update. Verification and an update are provisions as needed each time an individual submits an application.

Section 8.0 Technical Access and Security

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

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

The systems utilized are secure against unauthorized use through varying contingency procedures, which are in place to ensure that access control is under management following a strict need to know policy. Systems are secure against unauthorized use using layered, defense-in-depth security approach involving but not limited to managerial, operational and other technical controls, and security safeguards. Some of the systems operate in a secured environment and physical access is limited to System Administration, Database Administrators, Information Systems Security Officers, and other individuals that require access in order to perform their duties in managing, upgrading, and securing the system. For many systems, application administrators and users access the systems using a secure web interface. Unauthorized users have no access to system resources. Many systems require each user to acquire a unique login name and password as audit trails are under maintenance and monitoring to track user access and detect any unauthorized use. Some systems collect information from federal, state, local or tribal and emergency responder agencies who are U.S. citizens applying to use the Training and Exercise Programs. Users who access these types of systems usually fall into one of following categories:

- End users from federal, state, local and tribal fire and emergency response agencies known as "learners"
- Administrative users
- Specific systems administrators, database administrators, network engineers, etc.
- Admission personnel, including those located at Federal, State, or local jurisdictions which provide support to the system or program in there vicinity.

State and local training officials will have limited access to only the individuals included in his/her state or organizational training records and training plan.

8.2 Will Department contractors have access to the system?

Many of the systems currently under operation and those that are due to be in place in the near term are operating within a secure host and managing is a provision of contractor staff. In addition to operations and maintenance tasks, contractor staff has duties, which include, but are not limited to Application Development, Security Monitoring, and Information System Security Officer Duties. All contractors are subject to the vetting requirements for suitability and a background investigation in accordance with the DHS Sensitive Systems Handbook and contractors have signed appropriate non-disclosure agreements and agreed to handle the information in accordance with the Privacy Act of 1974, as amended. Only those contractors with a verified need to know and approved vetting will grant access to FEMA training and exercise systems.

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

All FEMA employees and FEMA contracted employees are required to completed FEMA Office of Cyber Security and Security Awareness Training. All contract employees are required to adhere to the Privacy Act/Confidentiality clauses as per terms of their contracts with FEMA.

Supplementary security related, and system specific training is set provisions for those with additional access requirements and security-related responsibilities, which will include, but is not limited to the following:

- OPM Rules of Behavior for Privileged Use of Information Technology Systems.
- On the job training on the receipt, processing, and disclosure of Privacy Act protected information handled in the Admissions and Housing Offices.

High-risk positions, which include the application developers and support personnel such as data base administrators and system administrators, are required to complete DHS Security Awareness training continually on an annual basis.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Yes. The required and completed C&A process dates for the many systems will vary, however without a verifiable and complete C&A, allowance, and inception of a new system will not be allowable.

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

On many of the systems, including, but not limited to all systems, user actions are required to be under recording within a log file and periodically reviewed to ensure that misuse of the system does not occur. Separation of duties is in place to ensure that users who have a functional administrative account in the system are incapable of altering/auditing the log files. Prior to acceptance of a new system, they are required to undergo a Certification & Accreditation (C&A) process.

In other instances, management controls will include periodic auditing of the system done in accordance with DHS System Security guidelines as established in the 4300 guidelines, as well as following current FEMA policies and procedures. Local system administrators govern the roles and rules established within their applications and, the auditing of user accounts are within the system requirements. Additionally, other measures provide safeguards, which include but are not limited to; Data access controls. This occurs via domains and workflows. A domain sets what data is accessible by an administrator and a workflow establishes what the administrator can do with that record in the database (e.g. Add Curriculum, Edit Online Content, etc.). To access such systems as the administrator or as an end user, the individual must have a valid and active account. Encrypted passwords are stored in the database and conform to the DHS password complexity rules. In this type of system, passwords must get an update every 90 days. System access ability is no longer allowable after three unsuccessful login attempts in one hour.

When end users enter their personal information, they use web server protection, using a 128-bit secure socket layer (SSL) certificate. Below are a list safeguards in addition to the aforementioned, which cover safeguards including but not limited to all systems:

- Student applications are not permissible outside the admission work area.
- Only Course Managers have permission to review applications for their own courses.
- Annual system control reviews using Security Test and Evaluation (ST&E), Security Assessment and SP800-53A Self Assessment.
- The use of managerial, operational and technical controls implemented to protect confidentiality, integrity and availability of a system and its information enforcing compliance requirements set by the DHS Sensitive Systems Handbook and FISMA
- Any control weaknesses identified will be remediated through the use of a Plan of Actions and Milestones (POA&M)
- Reviews occur in the admissions work area.
- Protection under the Computer Fraud and Abuse Act of 1986.
- Protection under the National Information Infrastructure Protection Act.
- Software programs that monitor and host and network traffic to identify unauthorized attempts to upload or change information or otherwise cause damage to users in the systems.
- Revocation control is under the control of Mass Care administrators, maintained by FEMA to deny access when unauthorized use detected.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

The risk of unauthorized access exists with any information technology system or document. To mitigate such a risk a series of security controls are in place to protect the confidentiality, availability, and integrity of the data, including role-based access controls which enforce a strict need to know policy.

The managerial, operational, and technical controls implemented to protect the confidentiality; integrity and availability of the systems and its information comply with the requirements of the DHS Sensitive Handbook and FISMA. These controls receive review annually through a Security Test and Evaluation (ST&E), Security Assessment and Annual SP800-53A Self Assessment. Any control weakness identified will receive remediation using a Plan of Actions and Milestones (POA&M) for the systems in use. All security controls are in accordance with DHS/FEMA security policy. The following are additional steps provided as cohesive measures to mitigate risk

- System users must agree to the system Rules of Behavior.
- The risk to PII are identified through a review and analysis of process flow and controls conducted by system developers, Information Systems Security Officer (ISSO) personnel, administrative personnel, and system owners.
- For many systems access to the work area is restricted, access to the system and database is tightly controlled, and handling of source documents is restricted.
- Information in the system or use of input to the system is not permissible outside of the work areas.
- On-the-job training is a provision for staff. Work processes receive monitoring to protect the privacy of student information.

Each user receives a unique login name and password. Official staff can utilize audit trails to provide necessary maintenance and monitoring which are tools available to track user access and detect any unauthorized use.

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 What type of project is the program or system?

There are many systems working independently of one another, which are part of a broader range of Information Technology. Many of the systems operate via web-based integrated systems, applications of design, development, evaluation, and improvement planning tools. Some of the systems provide Federal, State and local emergency response planners the timelines, templates, example documentation, and policy guidance needed to effectively manage and execute their exercise and training projects. Many of the systems are a development from the ground up by privately held companies that deliver innovative IT services and solutions to both domestic and international customers within the Federal Government and Commercial Markets. The systems enable users to prioritize, track, and analyze improvement plans developed from exercises and real-world events. Features include, but are not limited to Improvement Plan creation and maintenance, corrective action assignment and tracking, and reporting and analysis. Some system functionality follows the process described in HSEEP Volume III: Exercise Evaluation and Improvement Planning. Systems also support the processes by which exercise and real-world events can inform and improve exercise programs and other preparedness components. There are also systems developed by the Information Assurance Technology Analysis Center (IATAC) in support of U.S. Pacific Command (USPACOM) and selected by the Joint Staff as the joint exercise control tool of choice.

9.2 What stage of development is the system in and what project development lifecycle was used?

The Spiral development lifecycle model is one model, as well as DHS Information assurance and Infrastructure Protection IT Project Lifecycle to create many of the systems in use. While many other systems are currently in the operational stage and have been thoroughly evaluated and tested, other systems are still under development in coherence to FEMA Emergency Management Institute (FEMA/EMI) authority and determination. Routine maintenance occurs on a continuing basis to prevent large-scale failures and to minimize downtime.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

No, the projects do not employ technology, which may raise security concerns. Appropriate security measures are in place to ensure the confidentiality and integrity of PII. Risk assessments occur to identify current and emerging threats and mitigate any risks associated with the architecture of the aforementioned systems and projects.

Responsible Officials

<< ADD Privacy Officer/Project Manager>>

Department of Homeland Security

Approval Signature

____

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security