Privacy Impact Assessment
for the

Student Training/Exercise Application and Registration Records

DHS/FEMA/PIA-022

March 29, 2012

Contact Point
Eric M. Leckey
Privacy Officer
Federal Emergency Management Agency
Department of Homeland Security
(202) 646-3323

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Department of Homeland Security (DHS) Federal Emergency Management Agency (FEMA) collects, uses, maintains, retrieves, and disseminates Student Training/Exercise Application and Registration Records (STARRS) of sponsors, hosts, and attendees and conducts numerous training and exercise programs/systems, including conferences and seminars hosted by FEMA, in support of its mission. These programs collect personally identifiable information (PII) to register individuals for the respective training and exercise programs/systems; coordinate field exercises; and support the general administration of all registration, training, and exercise delivery and course evaluation for FEMA employees, contractors, members of the first responder community, as well as others. Where possible, FEMA's training and exercise programs/systems collect non-sensitive PII[1] such as contact information, business card information, biographies, and phone lists, as published in the FEMA Application and Registration Records for Training and Exercise Programs (ARRTEP)[2] Privacy Impact Assessment (PIA). Those include some programs within FEMA's Office of the Component Chief Human Capital Officer (OCCHCO), Federal Employee Knowledge Center (FEKC), and Learning Management System (LMS). Other programs, such as those sponsored by the National Training and Education Division (NTED), National Emergency Training Center (NETC), Emergency Management Institute (EMI), National Fire Academy (NFA), Center for Domestic Preparedness (CDP), and others from OCCHCO collect Sensitive PII (SPII)[3] such as Social Security Numbers (SSNs), performance information, financial information, name plus date of birth (DOB), and medical information because of the nature of the training or exercise program. This PIA documents how FEMA collects, uses, maintains, retrieves, and disseminates SPII in support of its training and exercise missions.

Overview

In support of FEMA's mission, the NETD, NETC, EMI, NFA, CDP, OCCHCO, and other regional and field offices, sponsor a range of training and exercise programs/systems for FEMA, contractors, members of the first responder community, as well as others.

Pursuant to Presidential Policy Directive (PPD 8) *National Preparedness;* Homeland Security Presidential Directive (HSPD) 5 *Management of Domestic Incidents;* Executive Order (E.O.) 13111 *Using Technology to Improve Training Opportunities for Federal Government Employee;* the Homeland Security Act of 2002; P.L. 93-498 the Federal Fire Prevention and Control Act of 1974; 6 U.S.C. § 748 *Training and Exercises*; and P.L. 93-288 the Robert T. Stafford Disaster Relief and Emergency Assistance Act as amended, FEMA collects, uses, maintains, retrieves, and disseminates SPII about the individuals who register or apply for FEMA training and exercise programs/systems and the organization employing or sponsoring these individuals, as well as information used to grant access to information technology (IT) systems that support these programs. FEMA's training and exercise programs/systems may also maintain information about the trainings and exercise events, which may be shared among

[1] DHS defines PII as any information that permits the identity of an individual to be directly or indirectly inferred, including any information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.
[2] Available at, http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-fema-arrtep.pdf.
[3] DHS defines Sensitive PII as personally identifiable information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

participants. The type and amount of SPII FEMA collected from individuals to facilitate their participation varies among training and exercise programs/systems. Some programs, such as those administered by NETC, may collect SPII such as financial information to facilitate payments and medical information to coordinate accommodations for individuals, while other programs collect only the PII necessary to register individuals, verify their identity, confirm their eligibility to participate in the training or exercise program, and facilitate participation in the program. Where possible, FEMA collects information directly from the applicant or registrant. This PIA focuses on programs that collect basic PII and that require SPII such as SSNs, performance information, financial information, name plus DOB, and medical information because of the nature of the training or exercise.

FEMA brings together partners from federal, regional, state, local, tribal, international, and non-governmental volunteer organizations, as well as the private sector, including firefighters, emergency medical services, emergency management agencies, law enforcement, and public officials for training and exercise programs/systems. These programs provide FEMA's employees, contractors, members of the first responder community, as well as others, with the opportunity to develop the situational awareness and skills necessary to respond quickly to all hazards. A complete list and description of training and exercise programs/systems covered by this PIA will be included in Appendix A of this PIA and will continue to be updated and maintained. Additionally, Appendix A includes FEMA training and exercise-related IT systems that may be either developmental or operational that are covered by this PIA and will also continue to be updated and maintained. All systems listed will go through the Certification and Accreditation (C&A) or Security Authorization processes as required by federal statute and DHS policy.

Registration Process

Individuals wanting to participate in a FEMA-sponsored training or exercise program and access supporting IT systems must first apply and register to do so. To facilitate this process FEMA generally collects information directly from the individual, and staff from the sponsoring organization verifies the individual's first responder status. In some instances, student information may also be provided indirectly by a state or local training agency when the course has been taken through that agency. Upon verification, the individual becomes a "registered user" and FEMA activates his/her user account. Typically, FEMA creates user names using the individual's email address, although another unique identifier may be used, and the individual selects their initial password as part of the registration process. A FEMA Support Service Administrator assigns access rights. If FEMA cannot confirm the first responder status of the individual, it cancels/prevents the registration and notifies the individual registrant of the cancellation by telephone and/or e-mail.

There are various levels of users with access based on official duties on a need to know basis. FEMA Support Services Administrators will have access to the modules of the system that they need in order to perform their official duties. FEMA budget offices and budget POCs have access to the student financial information needed to process payments. FEMA program offices will have access to reports that do not contain SPII.

Training Programs

FEMA's training programs include web-based training (WBT) and instructor-led training (ILT) courses. These courses relate to an individual's roles and responsibilities within a particular organization, system, or response plan and teach skills related to those roles and responsibilities. Training programs

prepare registrants to participate in training, exercises, tests, and actual emergencies related to response plans. The amount and type of PII, more specifically SPII, FEMA collects from participants in its training programs depends on the functionality and classification of the training and/or exercise program.

Evaluation and testing plays an important role in these training programs. FEMA components use WBT evaluation tools to collect data from both students and their supervisors to report on the effectiveness of their training programs. In addition, other WBT systems are used to support the ongoing administration of various elements of these training programs.

Exercise Programs

Exercise programs provide an environment for participants to schedule, plan, and perform simulated responses to a variety of possible real world hazards, incidents, and emergencies. Exercise programs validate the viability of one or more aspects of an emergency response plan. The amount and type of SPII FEMA collects from participants in its exercise programs depends on the functionality and classification of the exercise program.

Once admitted or registered, users can schedule and plan a training, exercise, or event. Some FEMA training and exercise programs/systems may also serve as a library to the first responder community. Registered users may upload and store After Action Reports (AAR), lessons learned, best practices, improvement plans, and other exercise/event-related documents into the system that supports a specific exercise. Other registered users of the system are able to access these documents to prepare for upcoming exercises/events in which they plan to participate. In addition, users are able to generate reports and graphs based on the improvement plan data posted to the system.

Access to reports and other records within the FEMA's training and exercise programs/systems are role-based. The Support Service Administrator (name varies from system to system) assigns access rights. There are various levels of users with access based on official duties on a need-to-know basis. Roles are generally designated Support Services Administrators, Budget Specialist/POC, and Program Specialist/Analyst. These access controls are documented in each system's security plan. FEMA retains this information pursuant to each program/systems record schedule.

FEMA's training and exercise programs/systems may share information with federal, regional, state, local, tribal, international, non-governmental/volunteer, and private sector organizations. FEMA shares this information to facilitate the development of training and exercise programs/systems, coordinate and track participation in training and exercise programs/systems (including transcript information), for statistical purposes to determine the nation's preparedness level, process reimbursement payments, and in some instances to provide housing to and transportation for students and other official guests. Information may be shared by providing information directly to applicants and students such as transcript information. Additionally, information may be shared using 128-bit encryption such as financial information to the U.S. Department of the Treasury (Treasury).

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

FEMA generally collects information for its training and exercise programs/systems pursuant to PPD 8 *National Preparedness;* HSPD 5 *Management of Domestic Incidents;* E.O. 13111 *Using Technology to Improve Training Opportunities for Federal Government Employee;* the Homeland Security Act of 2002; P.L. 93-498 the Federal Fire Prevention and Control Act of 1974; 6 U.S.C. § 748 *Training and Exercises*; and P.L. 93-288 the Robert T. Stafford Disaster Relief and Emergency Assistance Act as amended. Additionally, E.O. 9397 *Numbering System for Federal Accounts Relating to Individual Persons* authorizes the collection of SSN as a unique identifier; however, FEMA is currently developing an alternate unique identifier for use during application/registration and academic record keeping.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

FEMA training and exercise program/system records under this PIA are collected, used, maintained, retrieved, and disseminated in accordance with DHS/FEMA-011 General Training and Exercise Program Records System of Records Notice 76 FR 19107, April 6, 2011.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

In compliance with the Federal Information Security Management Act (FISMA) of 2005, and DHS Sensitive Systems Policy Directive 4300A, FEMA training and exercise IT systems covered by this PIA will go through the C&A or Security Authorization process and will be listed in Appendix A.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes, the records retention schedule has been approved by the FEMA Records Officer and NARA as Authority N1-311-88-2 1A and N1-311-88-2 2.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Those training and exercise programs/systems covered by this PIA, with information covered by the PRA, are listed in Appendix B.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

The following information is collected by FEMA's training and exercise programs/systems covered by this PIA:

Individual training registrant or exercise participant information

- Full name (first, middle, last);
- SSN or alternate unique identifier;
- DOB;
- Gender/sex;
- Race and ethnicity;
- U.S. citizenship (city and country of birth are collected for non-U.S. citizens);
- Home address or PO box including zip code;
- Home telephone number;
- Cellular telephone number;
- Work telephone number;
- Fax number;
- E-mail address;
- Military rank/prefix (if applicable);
- Employment status (e.g., full-time paid, part-time, volunteer, etc.);
- Position title;
- Primary responsibility;
- Category of position;
- Years of experience;
- Type of experience (such as incident command, administration/staff support, supervision, budget/planning);
- Professional certifications;
- Reference point of contact (POC);
- Reference POC phone number;
- Reference POC address;
- Relationship to the reference POC;
- Time zone; and

- Special assistance required (no or yes) (requested if housing is to be provided at the resident facility).

Agency, business, non-profit organization, military branch, or vendor information

- Organization type (e.g., federal agency, state or local government, tribe, private or non-profit);
- Organization classification (all career, all volunteer, combination);
- Organization address (including city, state, zip code and country);
- Organization identification number (e.g., fire department ID number);
- Organization phone number;
- E-mail address;
- Military service branch (if applicable);
- POC at the organization;
- Number of staff in the organization;
- Size of department;
- Size of the population served by the organization;
- DUN number;[4] and
- Course bid amount.

Training and exercise information

- Training/exercise name;
- Training/exercise type;
- Training/exercise date;
- Training/exercise mission;
- Training/exercise target capabilities;
- Reason for requesting access;
- Training/exercise scenario details;
- Training/exercise reports and other documentation;
- Venue/location;
- Exercise role (e.g., controller or player);
- Training/exercise prerequisites;

[4] Dun & Bradstreet verifies the existence of business entities globally. There is a separate DUNS number for each physical location of an organization. Visit https://eupdate.dnb.com/requestoptions.asp?cm_re=HomepageB*TopNav*DUNSNumberTab (Last accessed March 29, 2012).

- Course code;
- Exam answers;
- Evaluation survey questions and responses;
- Supervisor's name;
- Supervisor's mailing address;
- Supervisor's phone number;
- Supervisor's e-mail address;
- Password; and
- Security questions (2) - (varies per application/system and may or may not be required for resetting password created if user forgets password).

Stipend Reimbursement Payment participants' information

- Full name (last, first, middle);
- SSN;
- Business phone;
- Mailing address;
- Financial institution name;
- Routing number;
- Bank account title;
- Bank account number;
- Checking or savings account (check appropriate box);
- Odometer start;
- Odometer end; and
- Vehicle license number.

FEMA's training and exercise programs/systems that are listed in Appendix A: do not use commercial or publicly available data; utilize data mining to identify previously unknown patterns in the information collected in support of these programs; or use tools to analyze or produce new data.

2.2 What are the sources of the information and how is the information collected for the project?

FEMA collects, uses, maintains, retrieves, and disseminates the information in Section 2.1 to facilitate participation in FEMA training and exercise programs/systems, process stipend reimbursement payments, and organize academic records. FEMA collects this information directly from individuals, including training facility staff, seeking to register or apply to participate in FEMA's training and exercise

programs/systems. Individuals provide this information voluntarily. In some circumstances, state and local training agencies may submit applications on behalf of the individual(s) via hardcopy or electronically.

Generally, FEMA confirms status and/or eligibility of individuals requesting training or participation in an exercise via an application signed by the individual's supervisor or organization point of contact. Additionally, FEMA may confirm the status and/or eligibility of individuals requesting training or participation in an exercise by contacting the reference POC.

Training and exercise programs/systems collect SSN and financial information for the purpose of distributing reimbursements through Treasury or for processing invitational travel. Not all students will qualify or apply for stipend payments and/or travel payments. Additionally, SSN may be used as a unique identifier for matching of academic records with records maintained by other education institutions.

FEMA may collect information for its training and exercise programs/systems through paper applications, telephone registration, or through secure web-based forms. Not all training and exercise programs/systems use all of the aforementioned media for its information collection. FEMA's Records Management Division (RMD) approved forms that are used by FEMA training and exercise programs/systems are included in Appendix B of this PIA. Any training and exercise program/system that collects information using privacy sensitive technology such as biometric scanning or radio frequency identification (RFID) devices are not covered by this PIA.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

FEMA's training and exercise programs/systems associated with this PIA do not use commercial or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

FEMA collects information directly from individuals seeking participation in training and exercise programs/systems or by organizations represented by the individual. FEMA assumes the information provided is accurate. In some cases, Support Services Administrators for the organization sponsoring the training or exercise may confirm the applicant's identity and status as a first responder or Homeland Security official by contacting a reference provided during the registration process (such as by telephone or email). The registration approval process may include the review and approval of a training or exercise request by a FEMA region POC.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: Privacy risks associated with this system includes collecting more information than is necessary to register an individual for a training or exercise or process stipend reimbursements.

Mitigation: These privacy risks are mitigated by only collecting information necessary to complete the task and that enables FEMA to facilitate training and exercises that build, sustain, and improve the nation's capability to prepare for, protect against, respond to, recover from, and mitigate all hazards. Information such as SSN and financial information is used for academic recording (transcripts), and to reimburse or arrange invitational travel for training and exercise participants only. Information such as medical information is used to ensure physical capability to participate in exercises that are inherent to physical exertion. FEMA reviews these collections every three years to ensure continued legal authority and need of information.

Privacy Risk: Privacy risks associated with this system includes collecting, using, maintaining, retrieving, and disseminating inaccurate information on training and exercise program/system applicants and students.

Mitigation: These privacy risks are mitigated by collecting, where possible, information directly from the applicant or registrant. In a few cases, an organization my submit applicant information for their employee's to participate in conferences and/or seminars. It is assumed that the employer maintains accurate information for their employees. Additionally, FEMA may contact the applicant's employment POC to ensure information is correct.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

For training programs, FEMA uses the information it collects to create and update student records, enroll applicants into training courses, facilitate the completion of the training courses, provide applicants with completion certificates, track completions and failures, evaluate the effectiveness of training deliveries, collect instructor bidding/contract information, and communicate with trainees. In addition, FEMA uses the information it collects from trainees to confirm the individual's identity, establish their eligibility for system access, and to provide and monitor system security. FEMA may aggregate and review some of the information it collects for patterns and trends to determine the effectiveness of its training programs; however, FEMA does not use any PII for this purpose. Lastly, FEMA uses information such as sex, race, and ethnicity only for statistical purposes.

For exercise programs, FEMA will use the information to register exercise participants, facilitate registrant's participation in exercises, provide a collaborative working environment for exercise program development and project management, share improvement plans, after action reports, best practices, corrective actions and other documents resulting from completed exercises among emergency responders throughout the U.S., and communicate with exercise participants. FEMA uses the information to confirm the individual's identity, establish their eligibility for system access, and provide and monitor system security.

Training and exercise programs/systems collect SSN and financial information only for the purpose of distributing reimbursements through Treasury or for processing invitational travel. Not all students will qualify or apply for stipend payments and/or travel payments. Medical information is collected only to ensure that the applicant or student is physically able to participate in physically strenuous exercises.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

FEMA may search, aggregate, and review some of the information it collects for patterns and trends to determine the effectiveness of its training programs; however, FEMA does not use any PII for this purpose. FEMA may use search functions within its training and exercise database to locate trends such as how many law enforcement personnel from a certain area attended a specific training or exercise. Results are statistical in nature and do not produce information that is PII-related.

3.3 Are there other components with assigned roles and responsibilities within the system?

Other components may access training courses within a FEMA training system. In some cases systems may interact with a training system such as DHS HQ eDiscovery's technical connection with FEMA's Independent Study Database (ITSD) for certain training. FEMA does not assign other components with roles and responsibilities within FEMA's training or exercise systems with the exception when FEMA uses or purchases space on other federal entities' IT Technology system. In such rare cases, FEMA may permit the administrator of such system to have administrative rights for the sole purpose of help desk and troubleshooting support.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: A privacy risk associated with this system includes FEMA using the information it collects for training and exercise programs/systems for purposes other than that for which the information was collected.

Mitigation: This privacy risk has been mitigated because FEMA employs access controls, training, rules of behavior, and auditing. Only authorized users may access the information. Users must complete privacy and security training prior to receiving access to systems. Individuals accessing or using the system for purposes other than what is required for administration of training or exercise programs have restricted access to the system. Additionally, SPII information is only used and shared with an educational institution for academic record tracking, Treasury for payment related-issues, the OPM or a participant's employing agency for employment and career advancement purposes except when otherwise required by law.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

A Privacy Act notice is included on paper applications and websites that collect information for training and exercise programs/systems directly from the individual. Additionally, notice is provided

through this PIA and the DHS/FEMA-011 General Training and Exercise Program Records System of Records Notice 76 FR 19107, April 6, 2011.

For any system that collects information via telephone, FEMA staff will read a Privacy Act notice directly to the individual regarding the collection and use prior to collecting any information.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Individuals may decline to provide SSN, medical, or financial information, however, failure to provide this information may prevent eligibility and participation in certain training and exercises, or interfere with the ability of Treasury to process electronic payments provided by the stipend reimbursement program. Information regarding DOB, gender, ethnicity, and race is optional.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: A privacy risk associated with this system is that individuals may not know how FEMA training and exercise programs/systems will use their information, specifically, SSN, financial information, and medical information.

Mitigation: This privacy risk is mitigated through collecting registrant and applicant information directly from the individual as frequently as possible where they are provided a Privacy Act notice at the time of collection. Additionally, notice is provided through this PIA and the DHS/FEMA-011 General Training and Exercise Program Records System of Records Notice 76 FR 19107, April 6, 2011.

Privacy Risk: A privacy risk associated with this system is that individuals may not know how their information will be protected from inappropriate use and disclosure.

Mitigation: This privacy risk is mitigated through collecting registrant and applicant information directly from the individual where they are provided a Privacy Act notice at the time of collection. Additionally, notice is provided through this PIA and the DHS/FEMA-011 General Training and Exercise Program Records System of Records Notice 76 FR 19107, April 6, 2011.

Section 5.0 Data Retention by the project

5.1 Explain how long and for what reason the information is retained.

FEMA may retain all of the information listed in Section 1.1 for its training and exercise programs/systems, however, not all of the data elements are required for each training and exercise program/system.

In accordance with NARA authority N1-311-88-2 1A, admission applications and transcripts, including applications on students accepted for admission, student course completions, competency measures/scores, and transcript records have a retention period of 40 years. In accordance with NARA authority N1-311-88-2 2, student reimbursement records are retained for six years.

The retention period is based on the expected terms of employment of the applicant. The automated information is used to produce a transcript of training completed. Many of the courses have been recommended for college credit. Additionally, information is retained due to the highly sensitive nature of certain training and exercise programs/systems such as the chemical, ordnance, biological and radiological training which provides genuine toxic environments using chemical agents, biological, explosive, radiological, and other hazardous materials. Student reimbursement records are retained for financial auditing purposes.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: A privacy risk associated with this system is that FEMA may maintain the information collected for a longer period than is necessary.

Mitigation: Although there is always risk inherent in retaining PII for any length of time, the 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. This privacy risk is mitigated by purging or transferring records as required by the NARA-approved record schedule by the sponsoring FEMA training and/or exercise program.

Privacy Risk: Another privacy risk associated with this system includes keeping training and exercise information longer than what is approved by NARA.

Mitigation: This privacy risk is mitigated by utilizing advanced records management training, in addition to training offered by DHS and NARA, and utilizing advanced technology resources to improve records management practices and functionality.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Many of FEMA's training and exercise programs/systems are open to individuals throughout the emergency response community and FEMA shares the information it collects for its training and exercise programs/systems with a variety of external organizations.

Sponsoring organization/educational institutions (including state, local, and tribal):

FEMA may share general training and exercise information with a student's sponsoring agency such as a fire department, for the purpose of updating training and qualification records/requirements. Additionally, FEMA may share transcript information with educational institutions such as colleges, technical schools, and universities that may recognize certain FEMA courses as continuing education units or semester credit hours/units.

Federal Agencies:

FEMA shares SSN and financial information with Treasury for the purpose of distributing stipend reimbursements to qualified students. FEMA may share personnel information of federal employees with

U.S. Office of Personnel Management (OPM) and the federal employee's employing agency to be a part of an employee's personnel and performance files. Aggregated training/course information may be shared with other federal agencies for the purpose of course/exercise awareness of an employee's participation or as may be required by statute, regulation, or policy, but PII on individual employees will not be widely shared.

FEMA may share its training and exercise information outside of DHS via telephone, paper, and electronic means through the program/system's secure web interface. FEMA will include a letter to the organization, or execute an information sharing and access agreement such as a Memorandum of Understanding (MOU) with the external agency such as with another federal agency indicating that FEMA's Privacy Act records provided or transferred for use pursuant to applicable routine uses and that further disclosure of the records is not permissible.

This sharing is consistent with the purpose for which the information was collected and shared as outlined in the DHS/FEMA-011 General Training and Exercise Program Records System of Records Notice 76 FR 19107, April 6, 2011.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Routine use J allows DHS/FEMA to share training and exercise program information to a participant's employing agency/organization. This is compatible with the purpose of the original collection because a student's employer may require certain training and exercises programs to be completed as part of their duties as a first responders or to ensure compliance with federal statutes, such as completion of annual privacy act compliance training.

Routine use N allows DHS/FEMA to share SSN and financial information with Treasury. This is compatible with the purpose of original collection because Treasury requires SSN for tax reporting purposes and financial information to process and issue government funds such as stipend payments.

Routine use O allows DHS/FEMA to share academic records with OPM and with other educational institutions. This is compatible with the purpose of original collection because OPM maintains training information for federal employees and students both federal and non-federal may receive education credits for participation in FEMA courses.

6.3 Does the project place limitations on re-dissemination?

Information may not be re-disseminated outside of the sharing outlined in the DHS/FEMA-011 General Training and Exercise Program Records System of Records Notice 76 FR 19107, April 6, 2011 without the written permission of the individual or the FEMA Disclosure Office. Additionally, sharing of records provided to OPM may only be shared pursuant to the OPM/GOVT-1 General Personnel Records System of Records Notice 71 FR 35356, June 19, 2006. Records provided to Treasury may only be shared pursuant to Treasury 009-Treasury Financial Management System of Records Notice 70 FR 44190, August 1, 2005.

For all other external sharing of information, FEMA will either include a letter to the organization such as an educational institution, or execute an information sharing and access agreement such as a

Memorandum of Understanding (MOU) with the external agency such as with another federal agency indicating that FEMA's Privacy Act records provided or are being transferred for use pursuant to applicable routine uses and that further disclosure of the records is not permissible.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

FEMA maintains paper and electronic copies of all requests for academic records and the agencies response to the request. All information disseminated for the purpose of stipend reimbursements are retained in paper form and electronic form. Additionally, as identified in the DHS/FEMA-011 General Training and Exercise Program Records System of Records Notice 76 FR 19107, April 6, 2011, requests for information within the FEMA training and exercise programs/systems are made to the FEMA Disclosure Office who maintains the accounting of what records were disclosed and to whom under the Privacy Act and Freedom of Information Act.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: A privacy risk associated with this system includes information being shared for other purposes other than those for educational and payment processing.

Mitigation: This privacy risk is mitigated by FEMA limiting its information sharing to only educational institutions that are specifically requested by the student. In many cases, FEMA provides the academic records directly to the student upon their written request. The student may then share the information at their own discretion. FEMA's sharing of information for processing of reimbursement payments is limited to only what Treasury requires by statute to process Electronic Funds Transfer transactions. Further sharing of information is limited by the SORNs as discussed in Section 6.3 of this PIA. Additionally this information is accessible only to those with an established need-to-know. Individuals found accessing PII without an established need-to-know may be subject to disciplinary action including denial of access rights to records.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

Individuals may access their information via telephone by calling the Support Services Center (or Help Desk) for the FEMA component sponsoring the training or exercise program to which they have applied or seek to apply, or electronically via a web-based application. All individuals must provide information to authenticate their identity (user ID/Password) to access their information. Individuals may be required to answer a security question to access their information. 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, Office of Records Management, Federal Emergency Management Agency, Department of Homeland Security, 500 C Street, SW, Washington D.C. 20472.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

The procedures available to individuals may vary by program. First, individuals may call the Support Services Center (or Help Desk) supporting the training or exercise program that has the information that the individual seeks to correct. 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. Secondly, individuals utilizing web-based programs/systems may be able to correct their information themselves through the secure web interface.

Additionally, applicants and students seeking access to any record contained in the DHS/FEMA-011 General Training and Exercise Program Records System of Records Notice 76 FR 19107, April 6, 2011, or seeking to contest its content, may submit a request in writing to FEMA's FOIA Officer, Office of Records Management, Federal Emergency Management Agency, Department of Homeland Security, 500 C Street, SW, Washington D.C. 20472. The requirements for Privacy Act requests are documented in the DHS/FEMA-011 General Training and Exercise Program Records System of Records Notice 76 FR 19107, April 6, 2011.

7.3 How does the project notify individuals about the procedures for correcting their information?

FEMA notifies users of its training and exercise programs/systems of the procedures for correcting their information in a number of ways. Primarily, users receive notification from the specific training or exercise program to which they have registered. Typically, users are notified of how to correct their information by way of system training or system instructions provided for the specific IT system supporting the training and exercise program. In addition, users may receive such notification within the systems themselves, through on-screen help and/or hyperlinks. In addition, this PIA and the DHS/FEMA-011 General Training and Exercise Program Records System of Records Notice 76 FR 19107, April 6, 2011 provide notification to individuals regarding procedures for correcting their information.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: A privacy risk associated with this system includes that the individual may be unable to correct his/her information once it is provided to FEMA.

Mitigation: This privacy risk is mitigated by allowing an individual to correct his/her information: 1) through a telephone call to the appropriate Support Services Center (or Help Desk); 2) by accessing his/her record electronically, such as via a web-based interface using a user ID and password; and 3) by allowing access and correction through the procedures outlined in the DHS Privacy Act Regulations, 44 CFR Part 6 and 6 CFR Part 5.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

FEMA limits access to its training and exercise programs/systems to those users with valid, active accounts, with a user ID and a password that conforms to DHS password complexity rules. In addition, passwords must be updated every 90 days. Some programs/systems utilize access controls such that three unsuccessful login attempts within an hour result in the access rights for that user ID being suspended.

Many of FEMA's training and exercise programs/systems record user activity in a log file. FEMA periodically reviews these log files to safeguard against the misuse of such systems. The technical safeguards include a role-based access to these log files such that users whose access is administrative in nature cannot alter or audit the log files.

Management controls include the periodic auditing of systems in accordance with DHS Sensitive Systems Policy Directive 4300A, as well as 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, all FEMA systems are subject to a Privacy Compliance Review by the DHS and FEMA Privacy Offices to ensure compliance with this PIA and other supporting documentation.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

FEMA employees and contractors are required to receive initial and annual privacy training. Additionally, FEMA information technology system users are required to take initial and annual security training to ensure their understanding of proper handling and securing of sensitive information.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

DHS/FEMA utilizes role-based "need-to-know" access controls to ensure that the users of FEMA's training and exercise programs/systems have an appropriate level of access to the information contained therein. An individual's job title/role and reason for requesting access, which FEMA verifies this information prior to granting system access, determine the level of access the individual receives to FEMA's training and exercise programs/systems. In addition, the sponsor of each specific training and exercise program/system documents its access procedures and makes them available to "Help Desk" personnel to ensure appropriate customer service to registrants.

Contractor staff may provide system management, operations and maintenance, application development, security monitoring, and Information System Security Officer (ISSO) duties. All contractors are subject to the vetting requirements for suitability and a background investigation in accordance with the DHS Sensitive Systems Policy Directive 4300A 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 are granted access to FEMA training and exercise programs/systems.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

FEMA training and exercise programs/systems establish data sharing agreements with external entities using Interconnection Security Agreements (ISAs), MOUs, and Interagency Sharing Agreements. DHS Sensitive Systems Policy Directive 4300A establishes this requirement for DHS systems. An ISA is required whenever the security policies of the interconnected systems are not identical and the systems are not administered by the same entity/Designated Accrediting Authority (DAA). The ISA documents the security protections that must operate on interconnected systems to ensure that transmissions between systems permit only acceptable transactions. The ISA includes descriptive, technical, procedural, and planning information. The ISA also formalizes the security understanding between the authorities responsible for the electronic connection between the systems. The DAA for each organization is responsible for reviewing and signing the ISA.

Responsible Officials

Eric M. Leckey

Privacy Officer

Federal Emergency Management Agency

Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

APPENDIX A
Systems/Programs covered by STARRS PIA

Training Programs:

Center for Domestic Preparedness (CDP) Learning Management System

The Office of Protection and National Preparedness (PNP) National Preparedness Directorate (NPD) National Training and Education Division Center for Domestic Preparedness (CDP) Learning Management System (LMS) collects registration data, facilitates scheduling, travel logistics, course management, and course delivery for the CDP in Anniston, Alabama. CDP offers training courses in the following emergency responder disciplines: Emergency Management, Emergency Medical Services, Fire Service, Governmental Administrative, Hazardous Materials, Healthcare, Law Enforcement, Public Health, Public Safety Communications, and Public Works. The Chemical, Ordnance, Biological and Radiological Training Facility (COBRATF) at CDP offers the only program in the nation featuring civilian training exercises in a true toxic environment, using chemical agents. The advanced, hands-on training enables responders to effectively respond to real-world incidents involving chemical, biological, explosive, radiological, or other hazardous materials.

United States Fire Administration (Admissions) System

United States Fire Administration (USFA) Systems (USFASYS) performs management and operations functions for the USFA, Emergency Management Institute (EMI), and the National Emergency Training Center (NETC) campus as a whole at Emmetsburg, MD. USFASYS collects registration data, facilitates scheduling, travel logistics, course management, and course delivery information. Some of the courses offered by USFA may be used for college course/academic credits.

Exercise Programs:

Conferences:

APPENDIX B
Information Collections covered by STARRS PIA

OMB No.	Title of Collection
1660-0100	General Admissions Application (Long and Short) and Stipends Forms
1660-0032	National Fire Academy Resident Course Evaluation Form
1660-0046	EMI Independent Study Course Enrollment Application
1660-0029	Approval and Coordination of Requirements to Use the NETC Extracurricular for Training Activities
1660-0044	Emergency Management Institute Follow-up Survey
1660-0039	National Fire Academy Long-term Evaluation Form for Supervisors and National Fire Academy Long-term Evaluation Form for Students
1660-0034	Emergency Management Institute Resident Course Evaluation Form