Privacy Impact Assessment
for the

Application and Registration Records for Training and Exercise Programs

DHS/FEMA/PIA-016

March 3, 2011

Contact Point
Thomas R. McQuillan
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 Federal Emergency Management Agency (FEMA) sponsors, hosts and conducts numerous training and exercise programs in support of its mission. These programs collect personally identifiable information (PII) to register individuals for the respective training and exercise programs and to coordinate field exercises and provide training to FEMA employees, contractors, and members of the first responder and emergency management communities. This Privacy Impact Assessment (PIA) covers programs that collect basic PII but do not require sensitive PII such as Social Security numbers, dates of birth, financial and medical information for registration purposes.

Overview

The Department of Homeland Security Federal Emergency Management Agency's mission is to support our citizens and first responders to ensure that as a nation we work together to build, sustain, and improve our capability to prepare for, protect against, respond to, recover from, and mitigate all hazards.[1] In support of this mission, FEMA components such as the United States Fire Administration (USFA) and the Emergency Management Institute (EMI), which are housed at the National Emergency Training Center (NETC) facility, as well as the Protection and National Preparedness Bureau, and the National Processing Service Centers (NPSCs) sponsor a range of training and exercise programs for FEMA employees, contractors, and partners in the first responder and emergency management communities.

FEMA collects and maintains information about the individuals who register or apply for its training and exercise programs and the organization employing or sponsoring these individuals, as well as information used to grant access to IT systems that support these programs. FEMA's training and exercise programs may also maintain information about the trainings and exercise events, which may be shared among participants. The type and amount of PII FEMA collects from individuals to facilitate their participation varies among programs. Some programs, such as those administered by EMI and USFA, may collect sensitive PII such as financial information to facilitate payments and medical information to facilitate 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. However, this Privacy Impact Assessment (PIA) does not cover these types of training programs. This PIA covers programs that collect basic PII but do not require sensitive PII such as Social Security numbers, dates of birth, financial and medical information for registration purposes.

Through its training and exercise programs, FEMA brings together partners from state, local, tribal, regional, international, and nongovernmental/volunteer organizations, as well as the private sector, including firefighters, emergency medical services, emergency management agencies, law enforcement,

[1] Visit http://www.fema.gov/about/index.shtm for additional information.

and public officials. These programs provide FEMA's employees, contractors and partners with the opportunity to develop the situational awareness and skills necessary to quickly prevent, respond to, or mitigate all hazards affecting the people of the United States. A complete list and description of the training and exercise programs covered by this PIA is included in the Appendix of this document.

Registration Process

Individuals wanting to participate in a FEMA-sponsored training or exercise program and access supporting IT systems must first register to do so. To facilitate this process FEMA collects information directly from the individual and staff from the sponsoring organization verifies the individual's first responder status. 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. If FEMA cannot confirm the first responder status of the individual, it cancels the registration and notifies the individual registrant of the cancellation by telephone and/or e-mail.

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 tests, exercises, and actual emergencies related to response plans.

FEMA will retain this information for a maximum of five years after the completion of a specific training event.

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 PII FEMA collects from participants in its exercise programs depends on the functionality and classification of the exercise program.

Once registered, users can schedule and plan an exercise/event. The FEMA exercise systems 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 the upcoming exercises/events in which they will participate. In addition, users are able to generate reports and graphs based on the improvement plan data posted to the system. Access to reports within the FEMA's exercise systems is role-based. FEMA will retain this information for a maximum of 5 years after the completion of a specific exercise.

FEMA's training and exercise programs may share information with state, local, tribal, international, nongovernmental/volunteer organizations, and private sector organizations. FEMA shares this information to facilitate the development of training and exercise programs, coordinate, facilitate, and track participation in training and exercise programs, and for statistical purposes to determine the

nation's preparedness level.

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?

FEMA training and exercise programs require individuals to provide information during the registration process. This information may include the following data elements:

Individual Training Registrant or Exercise Participant Information

- Full Name (First, Middle, Last)
- Individual's unique User ID
- Sex
- Race and Ethnicity
- U.S. Citizenship (City and Country of birth are collected for non-U.S. citizens)
- Home Address or P.O. box including zip code
- Home Telephone Number
- Cellular Telephone Number
- Fax Number
- E-mail address
- Military Rank/Prefix (if applicable)
- Employment Status (e.g. full-time paid, part-time, volunteer, retired, etc.)
- Position title
- Primary responsibility
- Category of position
- Years of experience
- Professional certifications
- Reference Point of Contact
- Reference point of contact phone number
- Reference point of contact addresses

- Relationship to the Reference Point of Contact
- Time Zone

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 address (including city, state, zip code and country)
- Organization identification number (e.g. fire department ID number)
- Organization phone number
- Military Service Branch (if applicable)
- Point of Contact (POC) at the Organization
- Number of staff in the organization
- Size of the population served by the organization
- DUNS Number[2]

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
- Course code
- Exam answers
- Password

[2] Dunn & 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

- Security questions (2) – (Varies per application/system and may or may not be required for resetting password created if user forgets password)

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

FEMA collects the information in Section 1.1 directly from individuals seeking to register or apply to participate in FEMA's training and exercise programs. Individuals provide this information voluntarily. FEMA confirms the status and/or eligibility of individuals requesting training or participation in an exercise by contacting the reference point of contact.

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

FEMA collects the information to facilitate participation in its training and exercise programs. FEMA uses the information to register individuals seeking to participate in FEMA's training and exercise programs, to track performance, and to enable collaboration, information sharing, and full participation in the same. In addition, FEMA uses the information to confirm the status and/or eligibility of individuals requesting training or participation in an exercise by contacting the reference point of contact.

1.4 How is the information collected?

FEMA may collect information for its training and exercise programs through paper applications, telephone registration; or through secure web-based forms. Not all training and exercise programs will use all of the aforementioned media for its information collection.

1.5 How will the information be checked for accuracy?

FEMA collects the information directly from individuals who volunteer information; FEMA assumes the information is accurate. In many 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. The registration approval process may include the review and approval of a training or exercise request by a FEMA Region point-of-contact.

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

FEMA collects information for its training and exercise programs pursuant to 6 U.S.C. §. 748, "Training and exercises;", 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.

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

Privacy Risk: There is a risk of FEMA collecting more information than is necessary to register an individual for a training or exercise, verify that the individual is eligible to participate in the training or exercise, and/or facilitate communication relevant to the training or exercise.

Mitigation: FEMA mitigates this risk by limiting its information collection to only those data elements necessary to accomplish the uses in Section 2.1. As such, this PIA does not cover those FEMA training and exercise programs that collect, use, or maintain sensitive PII such as date of birth, Social Security number, financial, or medical information. Additionally, FEMA mitigates this risk during the PIA process through which the collection, use, and maintenance of PII are explained and privacy risks identified and mitigated. FEMA also mitigates this risk through the review of each form associated with these systems during the Paperwork Reduction Act (PRA) process, wherein the agency scrutinizes its collections of information from the public to avoid duplicative or unnecessary information collections.

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.

For training programs, FEMA will use the information to create and update student records, enroll applicants into training courses, facilitate the completion of the training course(s), provide applicants with completion certificates, track completions and failures, and communicate with trainees. 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. 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. 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 will also use the information to confirm the individual's identity, establish their eligibility for system access, and provide and monitor system security.

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

FEMA's training and exercise programs do not utilize data mining to identify previously unknown patterns in the information collected in support of these programs, nor do training and exercise programs use tools to analyze or produce new data.

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

FEMA's training and exercise programs do not use commercial or publicly available data.

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

Privacy Risk: There is a possible risk of FEMA using the information it collects for training and exercise programs for purposes other than that for which the information was collected.

Mitigation: FEMA mitigates this potential risk by employing access controls, training, rules of behavior, and auditing. Only authorized users may access the information, and users must complete privacy and security training prior to receiving access to systems. In addition, users must acknowledge and sign rules of behavior prior to accessing FEMA's information technology (IT) systems; rules of behavior include consequences for misuse of FEMA IT systems. In addition, to ensure accountability, auditing is preformed and all user activities undergo logging procedures. Lastly, support services and server administrative personnel undergo vetting in accordance with DHS Sensitive System Handbook 4300A policy, and receive 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?

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

3.2 How long is information retained?

FEMA retains its training and exercise information according to applicable NARA regulations. The length of retention may vary for each program/system, as each may have its own GRS record schedule or FEMA agency schedule. Generally speaking, training and exercise records for programs/systems covered under this PIA may be held for as little as three years and as long as five years from the "cut off," which will be either the date of the training or exercise event or the end of a calendar or fiscal year. Please see the Appendix for retention information specific to the systems covered by this PIA.

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

FEMA's training and exercise records retention is covered under General Records Schedules 1-29a(1), 1-29a(2), and 1-29b. FEMA Manual 5400-2M contains the Agency's record schedules.

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

Privacy Risk: There is a risk that FEMA could maintain the information it collects for a longer period than necessary. Although there is always risk inherent in retaining PII for any length of time, the data retention periods identified in the NARA schedule(s) are consistent with the concept of retaining data only for as long as necessary to support the agency's mission.

Mitigation: To mitigate the risk of FEMA retaining information beyond the approved retention period, the organization sponsoring each specific FEMA training and exercise program/system is responsible for the purging or transferring of records as required by the record schedule.

Privacy Risk: There is a risk that FEMA may keep its training and exercise information longer than what is approved by NARA.

Mitigation: To mitigate the risk of FEMA retaining its training and exercise information longer than what is approved by NARA, FEMA utilizes its advanced records management training, in addition to training offered by DHS and NARA and is advancing technology resources to improve its records management.

Privacy Risk: There is a risk that, generally, FEMA may retain its training and exercise records beyond what is necessary.

Mitigation: To mitigate the risk of FEMA retaining training and exercise information longer than necessary, records management training, which includes a focus on record retention, is required annually for all FEMA employees.

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?

FEMA shares its training and exercise program information with internal DHS components if there is a "need to know" and access the information. The purpose of sharing the information internally is to validate the identity of an individual requesting access to a training or exercise system. FEMA may also provide information on the training that an individual may have completed if the individual is employed by an agency or component of DHS. Section 1.1 includes the information that FEMA may share.

4.2 How is the information transmitted or disclosed?

Applicants may transmit information by paper (e.g., via fax), telephone (e.g., to the Help Desk), or electronically via the program/system's secure web interface. FEMA may share or disclose information internally via telephone (e.g., via the help desk) or electronically through the program/system's secure web interface.

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

Privacy Risk: There is a risk of unauthorized or improper disclosure of the information that FEMA collects and shares for its training and exercise programs.

Mitigation: FEMA takes several steps to mitigate this risk. First, for disclosure of training and exercise information via telephone, FEMA requires the caller to verify the answers to security questions prior to disclosing any information. Secondly, for electronic transmission and disclosure, FEMA utilizes audit trails and system logs which record each action by the user; FEMA only shares this information on a role-based, "need to know" basis; and when this information is shared it is password – protected, and encrypted using industry standard SSL –128 bit encryption used to protect data transmission. Lastly, before a user can transmit any information by fax, FEMA requires users to call the Help Desk servicing each program and have their user ID and password validated before receiving the fax number to enable the transmission of the information.

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?

As FEMA's training and exercise programs are open to individuals throughout the emergency response community, FEMA shares the information it collects for its training and exercise systems with a variety of external organizations. Such sharing is consistent with the purpose of FEMA's training and exercise programs applicable routine uses outlined in the Training and Exercise SORN, and supports the uses stated in Section 2.1.

To validate a user's identity so that he/she may become a "registered user" and receive an activated user account for a training or exercise system, FEMA may share the following training and exercise information with other federal agencies, offices, or departments; emergency response providers; and sponsoring state, local, and tribal officials and agencies:

- individual's full name (first, middle, and last); address; citizenship; training/exercise name or title; training/exercise date; cellular telephone number; mailing address; e-mail address; Military Rank/Prefix (if applicable); employment status (e.g., full-time paid, part-time, volunteer); position title; reason for requesting access; reference point of contact; and relationship to the reference point of contact.

FEMA may share the following training information on a "need to know" basis with:

- Federal agencies, offices, departments – individual's name, course title, and course completion date;
- Sponsoring State or local officials and agencies (including State Training Officers) – individual's name, organization address, email address, course code, course title, and completion date;
- Emergency response providers – individual's name, address, email address, course code, course title, and completion date;
- Member of Congress – individual's name, organizational address, email address, course code, course title, completion date, or course completions based on course code and state for first party information requests;
- Military personnel or training offices – individual's names, addresses, course codes, course titles, completion dates and continuing education units to award military credit for completed courses.

FEMA shares its exercise information with participants based on each user's role. FEMA may share the any of the following exercise information with federal agencies, office or departments; sponsoring state, local, and tribal officials and agencies; and emergency response providers on a "need to know" basis to facilitate participation and communication among exercise participants across participating organizations:

- individual's full name (first, middle, last); individual's professional certifications; individual's primary disciplines; organization/employer name; organization/employer address; organization phone number; cellular telephone number; fax number; e-mail address; training/exercise name or title; training/exercise type; training/exercise date; training/exercise mission; training/exercise target capabilities; training/exercise scenario details; venue/location; and exercise role (e.g., controller or player).

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, FEMA shares this information in accordance with the forthcoming DHS/FEMA Training and Exercise Program Records SORN being published concurrently with this PIA.

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

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 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 when transmitting information by paper..

For information transmitted electronically, proper security measures taken, including SSL 128-bit encryption when necessary.

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

Privacy Risk: There is a risk of unauthorized disclosure of FEMA's training and exercise information.

Mitigation: To mitigate this risk, FEMA limits its external sharing of its training and exercise information to those having a role-based "need to know," such as organization points of contact or other training/exercise participants. Furthermore, specific programs may allow users to restrict the amount of information that is available for sharing with other users, such as an exercise participant reducing the amount of information available in his/her profile. In addition, when FEMA shares training and exercise

data electronically, it minimizes the risk of unauthorized disclosure by utilizing secure measures such as secure web interfaces or 256-bit Advanced Encryption Standard (AES) technology.

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. FEMA provides notice of its information collection in several ways. First, FEMA provides notice through this Privacy Impact Assessment and the DHS/FEMA Training and Exercise Program Records SORN being published concurrently with this PIA. Secondly, FEMA provides notice via Privacy Act Statements, which are included on paper applications and websites that collect information for training and exercise programs. Lastly, for any system that collects information via telephone, FEMA staff will read a Privacy Notice regarding the collection to members of the public prior to collecting any information.

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, such a denial may affect the ability of the individual to register for a training course, participate in an exercise, or receive relevant resources such as timelines, templates, policy guidance and other design, development, evaluation and improvement planning tools, which are available to registered users of FEMA's training and exercise programs.

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

DHS will only use the information only for the purposes for which it was collected (i.e. to facilitate registration, participation, and record keeping pertaining to FEMA's training and exercise programs). Should an individual suspect information is being used beyond the given scope of the collection; they are encouraged to contact the FEMA Component Privacy Officer.

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.

Privacy Risk: There is a possible risk that individuals may be unaware that FEMA is collecting their PII.

Mitigation: FEMA mitigates this risk by providing notice through several mechanisms (as described in Section 6.1), including Privacy Act Statements and privacy notices at the point of collection.

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?

Individuals may access their information via telephone, by calling the Support Services Center 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 DC 20472.

7.2 What are the procedures for correcting 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. Lastly, the upcoming DHS/FEMA Training and Exercise Program Records system of records notice includes procedures for accessing and correcting exercise and training information.

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

FEMA notifies users of its training and exercise programs of the procedures for correcting their information 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 correction procedures during the training they receive on the uses and features of the specific IT system supporting the program. In addition, users may receive such notification within the systems themselves, through on-screen help and hyperlinks. In addition, this PIA the General Training and Exercise Program Records SORN being published concurrently with this PIA provide notification to individuals regarding procedures for correcting their information.

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

Redress for FEMA's training and exercise programs is provided as noted in 7.2 above.

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

Privacy Risk: There is a risk that the individual will not be able to correct his/her information once it is provided to FEMA.

Mitigation: FEMA mitigates this risk by allowing an individual to correct his/her information: 1) through a telephone call to the appropriate Support Services Center; 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 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?

DHS/FEMA utilizes role-based, "need-to-know" access controls to ensure that the users of FEMA's training and exercise programs and related 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 training and exercise systems. In addition, the sponsor of each specific

training and exercise program documents its access procedures and makes them available to "Help Desk" personnel to ensure appropriate customer service to registrants.

8.2 Will Department contractors have access to the system?

Yes. Contractor staff provides system management, operations and maintenance, 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 for those with additional access requirements and security-related responsibilities may include OPM Rules of Behavior for Privileged Use of Information Technology Systems, and on-the-job training on the receipt, processing, and disclosure of Privacy Act protected information handled in the Admissions and Housing Offices.

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 several training and exercise systems will vary, however new training and exercise systems cannot operate without a verifiable and complete C&A. Please see the Appendix for C&A information specific to the systems covered by this PIA.

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

FEMA limits access to its training and exercise 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 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 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.

Additionally, management controls include the periodic auditing of systems, in accordance with DHS 4300 System Security guidelines, 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.

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?

Privacy Risk: Given that FEMA's training and exercise programs and systems collect and share PII, including sensitive PII, there is a risk of unauthorized access to the information.

Mitigation: FEMA employs a variety of means to mitigate this risk. First, FEMA uses role-based access controls featuring unique usernames and passwords that enforce a strict need-to-know policy for its systems. Secondly, system users must agree to the "Rules of Behavior" that govern the system(s). Third, 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. Staff can utilize audit trails to track user access and detect any unauthorized use. Lastly, 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.

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?

FEMA has many training and exercise programs, with supporting IT systems, working independently of one another. FEMA's training and exercise programs include operational programs/systems, those that may be part of a toolset (e.g., the Homeland Security Exercise and Evaluation Program (HSEEP)), and in an effort to ensure continual improvement in providing capabilities to its partners, pilot programs/systems.

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

FEMA's training and exercise program IT systems may employ different development lifecycle models, such as the Spiral development lifecycle model, the Agile Development lifecycle model, or the DHS Information assurance and Infrastructure Protection IT Project Lifecycle.

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

FEMA's training and exercise programs do not utilize any technology which may raise unique privacy concerns beyond what is discussed in this PIA above.

Responsible Officials

Thomas R. McQuillan
Privacy Officer
Federal Emergency Management Agency
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

APPENDIX A
Systems covered by ARRTEP PIA
(*last updated on September 29, 2016*)

Training Systems:

National Shelter System-Computer Based Training (NSS-CBT) – The NSS-CBT is a web-based training for new users of the NSS. The training is designed 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. The NSS authority to operate is valid until 5/21/2012. FEMA will retain records for the NSS-CBT for 5 years after the completion of the program.

Exercise Systems:

Corrective Action Planning System (CAP) – The FEMA's Protection and National Preparedness Directorate sponsors the Corrective Action Planning (CAP) system. The purpose of this web-based tool is to enable Federal, State and local emergency response and homeland security officials to develop, prioritize, track, and analyze corrective action plans developed following exercises and real-world events. CAP is a component of the Homeland Security Exercise and Evaluation Program (HSEEP) Toolkit, a suite of interactive, online systems for exercise scheduling, design, development, evaluation, and improvement planning. The CAP authority to operate (ATO) is valid until 4/20/12. FEMA will retain records for CAP for 5 years after the completion of the exercise.

Design and Development System (DDS) – FEMA's National Preparedness Directorate sponsors the Design Development System (DDS). DDS is a project management tool and comprehensive tutorial for the design, development, conduct, and evaluation of exercises. The primary goal of the system is to help Federal, State, and local emergency response and homeland security officials resolve preparedness gaps or deficiencies in a systematic manner, ultimately strengthening national preparedness. DDS is a component of the Homeland Security Exercise and Evaluation Program (HSEEP) Toolkit. The DDS ATO is valid until 4/20/12. FEMA will retain records for DDS for 5 years after the completion of the exercise. FEMA is in the process of decommissioning this system. PrepToolKit (described below) will eventually replace DDS.

National Exercise Scheduling System (NEXS) – FEMA's National Preparedness Directorate sponsors the National Exercise Schedule (NEXS) System. The system provides consistent rules and means for scheduling exercises, advanced reporting features for planners to easily search and capture exercise information and basic information on each planned exercise. NEXS is a component of the Homeland Security Exercise and Evaluation Program (HSEEP) Toolkit. The NEXS ATO is valid until 4/3/11. FEMA will retain records for NEXS for 5 years after the completion of the exercise.

National Exercise Master Scenario Event List (NxMSEL) – FEMA's National Preparedness and Protection Directorate sponsors NxMSEL. NxMSEL is an automated system specifically designed to assist in master scenario event list (MSEL) management. During an exercise, NxMSEL provides tools for tracking progress and for reviewing, modifying, and releasing injects to the training audience. NxMSEL is a component of the Homeland Security Exercise and Evaluation Program (HSEEP) Toolkit. The NxMSEL ATO is valid until 6/10/11. FEMA will retain records for NxMSEL for 5 years after the completion of the exercise.

PrepToolKit – The FEMA National Preparedness Directorate, National Exercise Division (NED) operates the PrepTool Kit system. PrepToolKit is an expanded, modernized system that will eventually replace the functions of the Design and Development System (DDS) as well as provide additional functionality. The PrepToolKit supports the scheduling, design and development, evaluation, and improvement planning/lessons learned of training and exercise activities. PrepToolKit provides a space for registered users from the emergency response community to collaborate and exchange knowledge and documentation for training, exercises, and preparedness activities. NED manages the HSEEP, and PrepToolKit supports the overall mission of the program to provide a set of guiding principles for exercise programs and develop a common approach to exercise program management, design and development, conduct, and evaluation.