Privacy Impact Assessment
for the

First Responder Training System

July 16, 2008

Contact Point
Steve Schuetz
Federal Emergency Management Agency (FEMA)
National Preparedness Directorate
(202) 786-9569

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Department of Homeland Security (DHS) Federal Emergency Management Agency (FEMA) has developed the First Responder Training System (FRTS), FirstResponderTraining.gov. FRTS serves as a central access point to validate, FEMA-approved Weapons of Mass Destruction (WMDs) training and information. FRTS is an internet-based tool used to guarantee the provision of critical training for First Responders. The purpose of this PIA is to ensure the privacy risks associated with the collection of personally identifiable information (PII) are addressed for this new system.

Introduction

FirstResponderTraining.gov provides through a web-based interface training specific to FEMA-approved training and information specific to Weapons of Mass Destruction (WMD) and natural disaster events. It is used by Federal, State, and local emergency response and homeland security officials to train those personnel who will be charged with the duties of a first responder.

The Federal Emergency Management Agency (FEMA) pursuant to the DHS Preparedness Directorate, plans to use this system in part of a larger office-wide effort to translate National Exercise Program (NEP) outputs—such as findings, identified problems, recommendations, lessons learned, and best practices—into meaningful inputs for homeland security plans, programs, and budgets. Resources available on the site include multimedia videos which address WMD and terrorism topics as well as emergency response best-practices and peer-validated field experiences. Relevant reference materials such as training doctrine, standards, regulations, and other emergency response resources are available for viewing by authorized users.

FirstResponderTraining.gov serves as a central access point to validated, FEMA-approved Weapons of Mass Destruction (WMD) training and information for the following First Responder disciplines:

- Fire Service
- Law Enforcement
- Emergency Medical Services (EMS)
- Emergency Management
- Hazardous Materials (HazMat)
- Health Care
- Public Works
- Public Health
- Public Safety Communications
- Governmental Administration

FRTS provides terrorism training developed by the Federal Emergency Management Agency. Resources available on the site include multimedia videos, which address WMD and terrorism topics, emergency response best-practices, and peer-validated field experiences. Relevant reference materials such as training doctrine, standards, regulations, and other emergency response resources are available for viewing by authorized users.

Information that is collected from individuals is used to check employment of those individuals attempting to gain access to the FRTS. Individuals seeking access are generally required to be members of the First Responder Community (FRC) active in one of the aforementioned disciplines in order to receive access. Furthermore, once a user has been granted access, their unique username and password will be used to ensure that proper authentication is practiced for each user account in the system. Thus, collection of this information is used for the safeguarding of sensitive materials from access by unauthorized persons or entities.

Section 1.0 Information Collected and Maintained

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

1.1 What information is to be collected?

- First name
- Last Name
- Middle Initial
- Title
- Pilot Code (As the FRTS is currently in its Pilot program)
- Organizational Affiliation
- Supervisor contact information
- State
- Occupational credentials in the First Responder Community
- Email
- Phone number
- Fax number
- Street Address
- City
- Zip Code
- Answer to a security question – used for password resets, etc.
- Selected and unique username
- Password

Additionally, responses back from the respective employer's are maintained and employer contact information is collected that will be used to validate user access requests.

1.2 From whom is information collected?

The aforementioned information is collected directly from any individual who is pursuing an account on the FRTS. This will include DHS employees, contractors, state personnel, and local first responders. Generally, local first responders will be the personnel seeking access to the FRTS. Information is also gathered from employers contacted to validate user requests and identity.

1.3 Why is the information being collected?

The information identified above will be collected in order to properly authenticate user identities and therefore allow FRTS users access to For Official Use Only (FOUO), law-enforcement-based sensitive information. (Portal users must have the appropriate Public Trust clearance and valid "need-to-know" in order to access sensitive data located on the FRTS.) This information is authenticated via checks made by the requestor's employer as stated above.

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

Information is collected pursuant to Homeland Security Presidential Directive 8 "National Preparedness" (HSPD-8), the Homeland Security Act of 2002, the Privacy Act of 1974 (5 U.S.C. 552a), Executive Order 13111, Using Technology to Improve Training Technologies for Federal Government Employees and the E-Government Act of 2002 (Section 208).

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

Privacy risks were identified based on the unauthorized theft or disclosure of the information outlined above. Individuals employing social engineering techniques (e.g., spamming, etc.) could potentially use this information to locate individuals, identify individuals in sensitive positions, and masquerade as an individual to gain access to sensitive systems. To mitigate the risks associated with collecting PII, the FRTS has integrated robust security into its risk management plans and through the Certification and Accreditation processes routinely tests the security of FRTS. In addition, in accordance with the DHS Sensitive Systems Handbook, FRTS ensures effective security controls and authentication. By enforcing system policies and settings and strong passwords, the FRTS protects the privacy of data to promote or permit public access to the system and to protect the integrity of the data itself. Further, the FRTS has implemented best practices, such as auditing, to defend against misuse of the data and to monitor those with access to the information.

Section 2.0 Uses of the System and the Information

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

2.1 Describe all the uses of information.

The uses of the information described in section 1.1 are used for the purpose of identification and authentication for users who are both attempting to receive access to the FRTS and those attempting to retrieve their password in the event of a forgotten password. When a user registers for an account for the FRTS system they are requesting access to information that has been deemed sensitive by the United States Department of Homeland Security. For this reason, identification and authentication measures consisting of a username and password are required upon each sign in.

PII that is collected is used to verify upon registration that a person has a valid need for the account that is being requested. The request for occupational credentials as a member in the first responder community is meant to enable system administrators of FRTS to determine that only personnel who are qualified first responders receive access to FRTS. Verification of employment is received from the location where a registrant stated they worked before access is granted to the FRTS. This verification is performed by contacting the supervisor listed as the association to the requestor's organizational affiliation and confirming identity and occupation. Verification will be received via direct phone contact or e-mail.

Information that is collected from individuals is used to check employment of those individuals attempting to gain access to the FRTS. Individuals seeking access are generally required to be members of the First Responder Community (FRC) active in one of the aforementioned disciplines in order to receive access. Furthermore, once a user has been granted access, their unique username and password will be used to ensure that proper authentication is practiced for each user account in the system. Thus, collection of this information is used for the safeguarding of sensitive materials from access by unauthorized persons or entities. The FRTS maintains records of user requests for residential and mobile training courses as well as records of training provided to users through online courses.

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

The FRTS system does not have data mining functionality.

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

Current implementation of the FRTS is a pilot. A controlled set of users have been given a pilot code to register in the system. The system verifies the pilot code provided and considers supplied user and organizational information as acceptable for access to the system. As current accounts require access to the pilot code for a specific jurisdiction, the access to the pilot code as well as the verification process itself both assist in checking the accuracy of the information given by the requestor. Note: Pilot codes are only

given out to individuals requesting access by an individual designated as the State Administrative Agency point of contact. This action is put in place to add another layer of security to the requesting process.

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

Information collected can only be viewed by users with appropriate access and a verifiable need to know. Password fields are masked when being entered and are also encrypted inside the database so that no one other than the user can have access to said password. As confirmation of an individual's background is required for access to the FRTS, the FirstResponderTraining.gov application collects the minimum amount of personal information needed for such action.

Section 3.0 Retention

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

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

The only PII in the FRTS is user information entered by the registrant at the time of registration. User accounts and related training materials are not deleted for auditing purposes. As such, system data, including user account information and PII obtained from system users will be retained for a period of five years after the conclusion of the training programs offered by FRTS.

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

Yes; NARA has approved the retention schedule for FEMA and retention for the FRTS complies with the NARA approved record retention schedule contained in FEMA Manual 5400.2 (NARA GRS 1-29a(2) and GRS-1-29b). Information will be destroyed five years after completion of the FRTS program.

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

The information is retained indefinitely for auditing purposes and account maintenance (e.g., resetting passwords).

Section 4.0 Internal Sharing and Disclosure

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

4.1 With which internal organizations is the information shared?

Information may be shared DHS wide if there is a need to know within the scope of duties such as to demonstrate an individual has taken a particular training. PII is not shared outside of DHS, unless there is a demonstrated need to know and in compliance with the Privacy Act.

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

Information may be shared DHS wide if there is a need to know with in the scope of duties. The specific components within DHS are not predetermined.

4.3 How is the information transmitted or disclosed?

Information is accessible through the online web-portal found at http://www.FirstResponderTraining.gov. Users with the appropriate credentials can review information provided to their access level from any computer with an internet connection and an appropriate internet browser.

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

The identified risk associated with the disclosure of PII consisted of administrative or support personnel acting in a malicious and irresponsible fashion. This would include harvesting personal information illegally using administrative-level access. These actions are mitigated through the use of audit trails inherent in the system which logs each action performed. Logs are periodically reviewed to ensure that behavior is consistent with the Rules of Behavior set for the FRTS and suspicious activity is investigated. Additionally, individuals associated with FEMA are required to go through Security Awareness Training on an annual basis to ensure that procedures and security guidelines pertaining to sensitive information are properly understood.

Section 5.0 External Sharing and Disclosure

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

5.1 With which external organizations is the information shared?

Data collected from the FRTS may be shared with civil authorities during the registration process if in-depth background checks are required. Otherwise, information is only confirmed via the point of contact (supervisor) for the organizational affiliation listed by the registrant. In the future (2 to 3 years) it is possible that external systems will be able to verify user existence via a secure web server. Information will

be provided to organizations that are cited during the user registration process only. These organizations will include any police department, fire department, or other institution of first responders that are cited by registrants for the purpose of verification of employment. It should be noted that registered users cannot see each other's information. This privilege is explicitly granted to the system administrator.

This PIA will be updated to reflect external sharing when the process is introduced to the system.

5.2 What information is shared and for what purpose?

Information is not shared with external entities outside of the registration process and for verification of identity and determination of 'need-to-know' purposes.

5.3 How is the information transmitted or disclosed?

During the verification process, the point of contact listed for the organizational affiliation during the time of registration will be contacted so that the identity and role of the requestor (and the need to access the FRTS) can be confirmed. Information may be shared with aforementioned entities (police departments, fire departments, or other institution of first responders that are cited by registrants for the purpose of verification of employment). Transmission of data will be completed through the use of 128-bit SSL encryption if verification is performed via e-mail. Verification may also take place via direct phone communication.

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

Currently, no MOU is in place as no external entity receives information from the FRTS. In the future an applicable Memorandum of Understanding will be in place with all applicable external parties who will receive the information contained in the FRTS.

5.5 How is the shared information secured by the recipient?

When information is shared for the purpose of verifying of employment, external entities will be charged with not keeping specific records of the individuals who have had their background check completed. This negates the need for the securing of information and instead requires that information is destroyed or sanitized in a way that is appropriate for the type of information shared.

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

Administrative users for each State attend a four hour overview course that introduces the student and administrative sites. The student site is the area of the web-interface that deals with media and learning tools. The administrative site is simply the back-end where user administration and content management takes place.

During this review individuals receive pilot documentation explaining the functionality of the student site and administrative tasks State users can perform. Individuals also receive a Quick Reference Guide that can be used as a reference for the most common administrative tasks. Following the training, State users can schedule "just-in-time" training sessions covering their administrative tasks. Administrative users for each Training Partner attend a two hour overview of the student and administrative sites. They receive pilot documentation explaining the functionality of the student site and the administrative tasks Training Partners can perform. After the overview, Training Partners can schedule "just-in-time" training sessions, covering their administrative tasks.

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

The risk of privacy information being lost in the verification of employment is mitigated through the restriction of information that is shared with external organizations. Furthermore, the planned establishment of applicable MOUs will prohibit the storing of information by third parties in reference to the verification of employment. These items mitigate privacy concerns as they pertain to information sharing with third parties adequately.

Section 6.0 Notice

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

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

Notice is provided by the General Information Technology Access Account Records System (GITAARS) DHS/ALL-004, May 15, 2008, 73 FR 28139 System of Record Notice (SORN). Additionally, two messages available during user registration alert the user of the need for their contact information and its use. They are as follows:

"Registering on FirstResponderTraining.gov will allow you to access a variety of FEMA-approved training and content related to WMD topics. This content includes online training, videos, reference materials, best practices, lessons learned, a research library, and discussion forums."

"To confirm your employment as a first responder, we need to know the organization(s) through which you perform first responder role(s). Please enter search criteria below to try to find your work organization (police precinct, hospital, etc.) in our existing database."

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

Individuals who choose to register for the FRTS have the option to not register for the system. This action prevents them from being required to input any personal information. Should a person require access to the FRTS system, they will be required to complete the necessary registration form, including the fields requesting PII. This PII will be used to ensure that only users with a valid need have access to the FRTS system. Due to the sensitivity of the system, this denial of service is necessary.

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

Users implicitly agree that the information they are providing for registration to the FRTS system will be used to verify their identity and ensure that only properly accredited personnel receive access or recover passwords to the FRTS system. As this information will not be used for any other purpose, users are not provided the ability to select in what ways their information could be further shared.

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

Users will be explicitly informed that the information collected from them will be used to ensure their job function requires access to the sensitive information contained in the FRTS system. Therefore, the risks associated with the implicit system notification of the need of these items for registration of storing the items described and outlined in section 1.1. This will be done by inclusion and display of the Privacy Act of 1974, Section (e) during registration.

Section 7.0 Individual Access, Redress and Correction

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

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

Users are capable of reviewing all PII that has been provided by them by selecting the "Update Account Information" link found at the upper right hand area of the FRTS. Through this link, users are also able to correct or update any information that may have been originally entered incorrectly at the time of registration or information that may have changed since the time of registration.

7.2 What are the procedures for correcting erroneous information?

Two different processes are in place that allows a user to correct erroneous information they entered upon the time of registration. Users are allowed to log into the FRTS system and update their personal information using the "Update Account Information" link and corresponding fields that will populate the screen. Users also have the option of calling the Support Services Center that has been established for the FRTS system. When receiving an account restoration, if the user's identity has been verified through established means, the user may then request the Support Services Desk technician or senior technician to update their account information to reflect accuracy.

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

User manuals for the FRTS system have been distributed and made available to each prospective user. In these user manuals, the instructions for how to correct erroneous account information are available for easy reference to each user. Should a user have any questions about the information contained in the user manuals they are able to call the Support Services Center established for the FRTS and, after the user's identity is confirmed, update the necessary fields.

7.4 If no redress is provided, are alternatives available?

Due to the limited amount of personal information that is supplied by the individual during registration, the ease of the access of these files, and the capability of the user in correcting this information, no formal redress is necessary. The individuals who have access to the FRTS have access to their records and the capability to seek corrections or amendments at any time through administrative channels of the system or the Support Services Desk.

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

From within the FRTS application, users are allowed view and update their personal information and alternatively, the user can request that the correction be made by calling the FRTS Support Services Center. Privacy risks associated with redress include the collection of additional information on the individuals. Risks are mitigated by handling the information in the same way other data is handled.

Section 8.0 Technical Access and Security

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

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

K2Share Technical Teams (Database Administrators) – Administer access to the database. The K2Share team performs maintenance and ensures system performance.

K2Share Support Services Desk (Website Administrators) – A K2Share Support Services Desk representative has access to the administration screen in the FirstResponderTraining.gov website. Administrator account creation and the updating of user roles is also required of the K2Share Support Services Desk.

IT Specialist and Analyst (General access to the FRTS system) – Responsible for certifying system performance and integrity.

Administrators (General Access to Website) – Users with limited administrative rights to perform approvals, schedule classes, assign training, and run reports in the system for their area of responsibility.

Registered End Users (limited access to the system) – General users with limited access. End users can only access their personal information and see content determined by their role in the system.

8.2 Will contractors to DHS have access to the system?

Yes, contractors will have access to the system. FRTS is securely hosted and managed by contractor staff. In addition to operations and maintenance tasks, contractor staff performs application development, security monitoring and Information System Security Officer duties. All contractors are subjected to 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 will be granted access to the FRTS system

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

Separation of duties and privileges are in place that allow the administrators and support personnel of the FRTS system to determine the exact access given to users. The principle of "least privilege" is used as access is provided on a "business need only" basis. Only the access necessary for the adequate completion of the job function is given to any user.

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

A registration process is in place to ensure a user is given the appropriate roles and content visibility. Administrative accounts are given their roles and responsibilities based on their needs. These roles are given certain access. Roles are documented in the System Design document.

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

For individuals leaving the organization, changing roles, or having system access revoked due to unfavorable conditions, user accounts and passwords will be disabled immediately by the appropriate administrator (e.g., FRTS System Administrator).

When accounts have been inactive for a period of 180 days they will be automatically disabled by the system via an administrative script. (This script may also be run manually when deemed appropriate.)

The script operates by automatically examining every user account in the database and runs as an overnight process at 12:00 AM CST. For auditing purposes, accounts are never completely erased.

Passwords for user accounts will automatically expire after a 90 day period. The system will require the user to reset their password before re-entry into the system will be allowed.

The Information System Security Officer (ISSO) will be required to certify annually to the Information System Security Manager (ISSM) that no unauthorized user accounts remain outstanding in the system.

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

All user actions are logged and periodically reviewed to ensure that misuse of the system does not occur. Separation of duties is in place to ensure that users who have a functional administrative account in the system are incapable of altering/auditing the log files.

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

Users who require access to FOUO information will be required to take the DHS Security Awareness Training annual refresher training that outlines "best-practices" in terms of practice and privacy. This provides privacy training to the users who will have any sort of an administrative account as they will require privacy training due to the fact they will be able to access user information.

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

An official Authority to Operate is currently being pursued through the Certification and Accreditation process and Office of the Chief Information Officer.

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

The Privacy Office stated that privacy concerns inherent in the contract would be suitable for inclusion in this document. As such, references to privacy acts and standards have been compiled below:

The Office for Domestic Preparedness (ODP) is part of the Department of Homeland Security Federal Emergency Management Agency (FEMA). The mission of ODP is to improve the capacity of State and Local entities to respond to acts of terrorism, particularly those involving WMDs. ODP accomplishes this mission through equipment acquisition assistance, technical assistance, training, and exercise support. The FRTS is a web-based training tool used to this end.

As Administrators will have the ability to access personal information for all users, it was identified in the privacy assessment of the system that administrators must receive a Public-Trust Clearance to be able to perform their job function. The adherence to this standard has mitigated this privacy concern. Public Trust clearance requires a minimum background check, including criminal, credit, and employment to ensure that persons given the Public Trust designation are trustworthy.

Section 9.0 Technology

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

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

The FRTS is a combination of software created by designated contractors and commercial off-the-shelf (COTs) software applications. The COTs applications are Plateau (LMS), Jive (forums), MS-SQL (Database), Oracle (Database), and Tomcat (Web Server). Every other element of the FRTS is original code written by the designated contractor.

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

Initial stages of the design phase recognized the need to ensure the integrity and security of the sensitive information to be collected. Decisions about the system design were based on the need to control access to the system resources as well as the content. A role-based system was implemented to ensure privacy controls and content access. This dynamic set of roles can be enhanced as the need for more granular access is identified.

9.3 What design choices were made to enhance privacy?

Role-based access ensures that only users with authorization have access to sensitive or PII.

Conclusion

Account and access security was evaluated in order to ensure controlled and powerful personalization and customization software functionality, as such; the system has various user access levels to mitigate privacy risks. FRTS officials and administrators follow the same policy and guidelines for approved accounts and determining access groups. Only those individuals with a need to know and proper authorization have access to an administration user account will be able to view personal information of other users.

Responsible Official

John A. Sharetts-Sullivan

FEMA Privacy Officer

Department of Homeland Security

Approval Signature Page

Original signed and on file with the DHS Privacy Office.

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security