



Homeland Security

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy

Privacy Threshold Analysis

Version date: June 10, 2010

Page 1 of 7

PRIVACY THRESHOLD ANALYSIS (PTA)

**This form is used to determine whether
a Privacy Impact Assessment is required.**

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Rebecca J. Richards
Director of Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 703-235-0780

PIA@dhs.gov

Upon receipt from the component Privacy Office, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, www.dhs.gov/privacy, on DHSConnect and directly from the DHS Privacy Office via email: pia@dhs.gov, phone: 703-235-0780.



PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Date Submitted for Review: May 16, 2012

Name of Project: National Emergency Family Registry and Locator System

System Name in TAFISMA: National Emergency Family Registry and Locator System

Name of Component: Federal Emergency Management Agency (FEMA)

Name of Project Manager: Fred Amini

Email for Project Manager: Fred.Amini@fema.dhs.gov

Phone Number for Project Manager: 540-722-8496

Type of Project:

Information Technology and/or System.*

A Notice of Proposed Rule Making or a Final Rule.

Form or other Information Collection.

Other: <Please describe the type of project including paper based Privacy Act system of records.>

* The E-Government Act of 2002 defines these terms by reference to the definition sections of Titles 40 and 44 of the United States Code. The following is a summary of those definitions:

•“Information Technology” means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. See 40 U.S.C. § 11101(6).

•“Information System” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

Note: for purposes of this form, there is no distinction made between national security systems or technologies/systems managed by contractors. All technologies/systems should be initially reviewed for potential privacy impact.



SPECIFIC QUESTIONS

1. Describe the project and its purpose:

FEMA established the National Emergency Family Registry and Locator System (NEFRLS) system in compliance with the DHS Appropriations Act of 2007 to help family members separated after an emergency or major disaster to find and communicate with one another.

The NEFRLS system is a nationally accessible and recognized system for individuals who have been displaced by a Presidentially-declared disaster or emergency to voluntarily enter personal information into an Internet accessible database that their family can access to help locate one another. The system also allows adults who are parents or guardians of displaced children to register their child in NEFRLS. NEFRLS offers a mechanism for voluntary registration of displaced people over the Internet or phone. After registering in the system, displaced individuals can leave a message and/or current contact information for family. The NEFRLS system allows individuals to search for displaced persons via the Internet or phone after they have completed an identity verification and authentication process. A person searching the system is only able to view a displaced person's recorded information if that displaced person has included the searcher on their list of individuals authorized to view the record.

FEMA has made several enhancements to the NEFRLS system. This PTA documents the changes to NEFRLS as of November 2010. Furthermore, the July, 25, 2011 NEFRLS Privacy Impact Assessment update references an update to NEFRLS that involved sharing information with the FEMA Disaster Assistance Improvement Program (DAIP) system. This update to the system never occurred.

2. Status of Project:

This is a new development effort.

This is an existing project.

Date first developed: May 3, 2007

Date last updated: November 2, 2010 (NEFRLS Version 2.0)

The following changes were included in NEFRLS Version 2.0

NEFRLS Version 2.0 adds: 1) a Law Enforcement Officer (LEO) module; and 2) the ability to send Short Message Service (SMS) text messages.



Privacy Threshold Analysis

Version date: June 10, 2010

Page 4 of 7

The LEO module provides FEMA staff the ability to assist law enforcement in locating missing/displaced survivors of a Presidentially-declared disaster or emergency by linking them to information on missing persons who may have registered in NEFRLS. LEO only requests a survivor's information within NEFRLS for the purpose of reuniting family and friends who may have contacted their local law enforcement office or submitted a Missing Persons Report via email to FEMA. LEOs do not access or search the system, but rather are provided information on specific requests by FEMA staff. Prior to executing a LEO-requested search for a possible registrant, the FEMA representative requests a copy of the Missing Persons Report and identifying information on the LEO in order to facilitate identity verification and their status as a member of law enforcement. The report FEMA staff provides to a law enforcement official contains the registrant's full name, gender, address, and disaster incident information (e.g., Hurricane Katrina, Mississippi Flooding etc). FEMA logs in NEFRLS that they disclosed a particular record to a specific LEO.

The SMS functionality allows registrants to receive a short SMS text message from family with whom they have elected to share information in their record in the NEFRLS system. The collection of SMS information is used exclusively for delivering SMS messages to registrants. The cellular phone number is collected from the displaced person during the registration process. An individual initiates the search for a displaced individual in the NEFRLS system. Once a searcher has gained access to a displaced person's profile the searcher can submit a short message to the displaced individual by typing the text in the designated SMS text box field and clicking submit. The NEFRLS system then sends the SMS message to the cellular phone number provided by the displaced person. FEMA does not share the actual cellular phone number with others.

3. From whom do you collect, process, or retain information on: (Please check all that apply)

- DHS Employees.
- Contractors working on behalf of DHS.
- The Public.
- The System does not contain any such information.

4. Do you use or collect Social Security Numbers (SSNs)? (This includes truncated SSNs)



Privacy Threshold Analysis

Version date: June 10, 2010

Page 5 of 7

No.

Yes. Why does the program collect SSNs? Provide the function of the SSN and the legal authority to do so:

<Please provide the function of the SSN and the legal authority to do so.>

5. What information about individuals could be collected, generated or retained?

NEFRLS Version 2.0 collects three categories of information from each displaced individual who voluntarily registers in NEFRLS:

1. Registrant Information: Full Name, Suffix, Date of Birth, Gender, Current Phone, Current Address, Pre-Disaster Address, Name of Current Location, Names of up to seven friends/family members authorized to view the registrants' information, Identity Authentication Approval or Non-approval (Identity verification and authentication process through ChoicePoint), System specific username and password, and Personal Message
2. Family/Household Information: Full Names of family/household members traveling with the registrant, and Personal Message viewable by searchers
3. Searcher Information: Full Name, Permanent Address, Phone, Date of Birth, Identity Authentication, and System specific user name and password.

NEFRLS version 2.0 collects the following additional information from individuals requesting to receive information via SMS messages:

- Cell Phone Number, Cell Phone Carrier, and E-mail Address.

NEFRLS version 2.0 collects the following information from Law Enforcement Officers:

- Law Enforcement Official's Title, First Name, Last Name, Gender, Badge Number/Law Enforcement License ID Number, Agency Name, City, County/Parish, State, Zip Code, Contact Phone, Contact E-mail, Supervisor Name, Supervisor Contact Number, Supervisor Contact E-mail, Agency City, Agency County/Parish, Agency State; and Verification Data (The verification process includes a confirmed box to be checked for successful verification of LEO's identity and status via telephone by NEFRLS Administrator).

6. If this project is a technology/system, does it relate solely to infrastructure? [For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)]?



- No. Please continue to the next question.
 - Yes. Is there a log kept of communication traffic?
 - No. Please continue to the next question.
 - Yes. What type of data is recorded in the log? (Please choose all that apply.)
 - Header.
 - Payload Please describe the data that is logged.
- <Please list the data elements in the log.>

7. Does the system connect, receive, or share Personally Identifiable Information with any other DHS systems¹?

- No.
- Yes.

8. Is there a Certification & Accreditation record within OCIO's FISMA tracking system?

- Unknown.
- No.
- Yes. Please indicate the determinations for each of the following:

- Confidentiality: Low Moderate High Undefined
- Integrity: Low Moderate High Undefined
- Availability: Low Moderate High Undefined

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

Date reviewed by the DHS Privacy Office: May 17, 2012

¹ PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in TAFISMA.



Privacy Threshold Analysis

Version date: June 10, 2010

Page 7 of 7

Name of the DHS Privacy Office Reviewer: Brian E. Anderson

DESIGNATION

This is NOT a Privacy Sensitive System – the system contains no Personally Identifiable Information.

This IS a Privacy Sensitive System

Category of System

- IT System.
- National Security System.
- Legacy System.
- HR System.
- Rule.
- Other:

Determination

- PTA sufficient at this time.
- Privacy compliance documentation determination in progress.
- PIA is not required at this time.
- PIA is required.
 - System covered by existing PIA:
 - New PIA is required.
 - PIA update is required.
- SORN not required at this time.
- SORN is required.
 - System covered by existing SORN: DHS/ALL-004 General Information Technology Access Account Records System (GITAARS) of Records (September 29, 2009, 74 FR 49882) and DHS/FEMA-001 National Emergency Family Registry and Locator System (NEFRLS) System of Records
 - New SORN is required.

DHS PRIVACY OFFICE COMMENTS FEMA WILL UPDATE THE NEFRLS PIA TO REMOVE LANGUAGE REGARDING AN ASPECT OF NEFRLS THAT WAS NEVER IMPLEMENTED.