Privacy Impact Assessment
for the

National Emergency Family Registry and Locator System (NEFRLS)

August 27, 2009

Contact Point
Waddy Gonzalez
Mass Care, Unit Chief
Department of Homeland Security
Federal Emergency Management Agency
202-212-1077

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

Abstract

The Federal Emergency Management Agency (FEMA) operates the National Emergency Family Registry and Locator System (NEFRLS). NEFRLS is a web-based system which, when activated, collects information from individuals for the purpose of reuniting family and household members that have been displaced as a result of a Presidentially-declared disaster or emergency. FEMA conducted this Privacy Impact Assessment (PIA) because the system collects personally identifiable information (PII).

Overview

During Hurricane Katrina, displaced individuals experienced numerous difficulties in reuniting with family and household members. As a result, Congress mandated that FEMA establish the National Emergency Family Registry and Locator System (NEFRLS) in the Post-Katrina Emergency Management Reform Act (PKEMRA), Pub. L. 109-295, section 689c. FEMA holds primary responsibility for the NEFRLS to help reunite families separated after an emergency or major disaster declared by the President pursuant to the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act) 42 U.S.C. §§ 5121-5207.

NEFRLS is a web-based system which when activated during a Presidentially-declared disaster or emergency, enables FEMA to provide a nationally accessible and recognized system that allows adults displaced from their home or pre-disaster residence ('registrants') to voluntarily register to facilitate the reunification of their family and household members. Individuals who are searching for displaced family, friends, or household members may also register in the system ('searchers'). Adults registering or searching for a displaced child under the age of 21 will be directed via an Internet link to the National Emergency Child Locator Center (NECLC) or through a referral to the NECLC 800 number. Additionally, as provided for in PKEMRA, medical patients that have been displaced due to a major disaster or emergency will have access to and can voluntarily register in the system. No medical information is solicited by the program or the NEFRLS system.

The registrant can register in one of two ways during a disaster. The first is via the NEFRLS 800 number by which an operator at the Texas National Processing Center will take their information over the phone. The second option is via the internet through www.FEMA.gov or directly at https://asd.fema.gov/inter/nefrls/home.htm. Once a registrant has contacted FEMA NEFRLS either via the website or telephonically, a standard NEFRLS Privacy Act Statement is either viewable or read to the registrant. After acknowledgement of the Privacy Act statement, the registrant provides PII to NEFRLS including, among other things, pre-disaster and current location information. Once this PII is provided, the registrant is sent to a third party for identity authentication. If the registrant successfully answers 3 of the 4 multiple choice questions unique to their identity, the registrant is may setup an account accessible by username and password. If the registrant decides not to setup a username and password to access their account, the registrant will need to go through the identity authentication process each time to access their account.

Once the registrant's identity is authenticated, the registrant provides limited PII on any household or family members traveling with them. The registrant can then identify up to seven individuals ('searcher') that they authorize to view their PII, including their current location and contact phone numbers. The registrant provides the first name and first letter of the last name of the authorized searcher. The registrant also has the ability to designate which information (e.g., contact information, personal message, and/or

household members traveling with the registrant) the searcher is able to view. In addition to access provided to authorized searchers, information entered in NEFRLS by the registrant will be available upon written request to those governments agencies, non-government agencies, federal, state, local and tribal law enforcement officials, and non-profit organizations specifically responsible for locating and reuniting family members displaced by a disaster. Information will be delivered to these requestors by paper copy via First Class Mail requiring a signature.

Individuals who are searching for family, friends or household members may also register in NEFRLS ('searchers'). Searchers, follow the same registration process as 'registrants' and are also required to be authenticated through a third party. Once the searcher's identity is authenticated through the third party services or by providing a valid username and password, the searcher then enters the first and last name; country; state; and city of the displaced person ('registrant'). NEFRLS then provides a list of name matches. When there are multiple name matches, the searcher is requested to refine their search by providing the address, primary contact phone number, date of birth and/or gender. NEFRLS will provide new results based on the refined details. Once the searcher identifies for the correct registrant, NEFRLS will verify that the searcher is on the registrant's viewer list. If the searcher is not on the authorized viewer list, then access to the registrant's information will be denied. If the searcher is on the registrant's viewer list, the searcher will be able to view information designated by the registrant.

For those who are reporting a missing child or searching for a missing child, the guest is provided a link to the National Emergency Child Locator Center (NECLC) (www.missingkids.com) website.

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 a part of the program, system, rule, or technology being developed.

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

NEFRLS collects three categories of information; registrant information, family/household information, and searcher information. The following is detailed information collected and maintained in NEFRLS:

Information from or about the individual registering in the NEFRLS ("registrant") includes:

- Full Name (First, Middle, Last)
- Suffix
- Date of Birth
- Gender
- Current Phone
- Alternate Phone
- Current Address
- Pre-Disaster Address
- Name of Current Location, (i.e., shelter, hotel, or family/friend's home)
- Traveling with Pets (Yes or No)

- First names and last name initial of up to seven friends/family members authorized to view the registrants' information and any viewing limitations including permission to view contact information, view messages, or view members traveling with registrant.
- Identity Authentication Approval or Nonapproval: FEMA maintains the fact of the authentication but the answers to the questions provided to the third party organization are not maintained by DHS/FEMA.
- System specific username and password
- Personal Message (may consist of up to 300 characters intended for designated family or household members to read)

Information about the family/household members traveling with the registrant in the NEFRLS includes:

- First Name
- Last Name
- Personal Message: Full names of family or household members that the registrant in the NEFRLS has permitted to view his or her information and/or message. (The registrant can create a personal message which may consist of up to 300 characters for listed, designated family or household members to read).

In addition to the registrant information requested, information about the individual searching the NEFRLS for a registrant or family/household member (searcher) includes:

- Full Name
- Permanent Address
- Phone
- Alternate Phone
- Email
- Date of Birth
- Identity Authentication Approval or Nonapproval: FEMA maintains the fact of the authentication but the answers to the questions provided to the third party organization are not maintained by DHS/FEMA.
- System specific username and password

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

There are three sources of information: the first is adults, including medical patients, who have been displaced as a result of a Presidentially-declared disaster or emergency under the Stafford Act and register their information into the system. The second source is individuals searching the database, who will be required to provide personal information for the purpose of verifying and authenticating their identity before they can access any information about an adult displaced individual who has submitted their PII in the system. The third source is the third party authentication service that is providing authentication services. As noted above, DHS/FEMA does not receive the answers to the authentication questions, but rather receives the "approved" or "not approved" from the third party authentication service.

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

NEFRLS collects the information for the purpose of facilitating the reunification of family members that have been displaced after a Presidentially-declared major disaster or emergency. NEFRLS allows displaced individuals to provide their current contact information and leave a brief message for their family and/or household members. The information collected also allows authorized individuals to search for family or household members that may have evacuated due to a major disaster or emergency. This information will also assist Government agencies, non-government agencies, federal, state, tribal and local law enforcement officials and non-profit organizations such as the Office of Juvenile Justice and Delinquency Prevention, Department of Health and Human Services, U.S. Department of Justice, FBI's Crimes Against Children's Unit, U.S. Department of Justice U.S. Marshals Service, The American Red Cross, and the National Center for Missing and Exploited Children, in reuniting displaced individuals (including medical patients) with their family members.

1.4 How is the information collected?

Information is collected directly from individuals in one of two ways: (1) electronically (via the Internet) by individuals (who have been displaced as a result of a Presidentially-declared disaster or emergency or who are searching for displaced family or friends) who voluntarily register in to the system or (2) through an 800 number where individuals voluntarily call and provide a call center representative with the authorization to enter their information into the electronic system. Information from the third party authentication service is provided electronically directly from the service.

1.5 How will the information be checked for accuracy?

In addition to information collected directly from individuals, the individual must review confirmation pages to increase the accuracy of the data being entered. NEFRLS registrants and searchers are asked to review their information and confirm it on a second page before final submission. After registering, the registrant can review and make any needed corrections to their information by selecting the "Update My Registration" option on the NEFRLS homepage.

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

FEMA is authorized to collect this information under Section 689c of PKEMRA in Title VI of the DHS Appropriations Act of 2006 (PKEMRA), Pub. L. 109-295, 120 Stat. 1355 at 1451, and the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act), 42 U.S.C. §§ 5121-5207.

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

The amount of PII collected by FEMA can increase risks for misuse of this information. For example, compromise of PII can result in harm (e.g., identity theft) and/or embarrassment to an individual. To mitigate these risks, FEMA collects the minimum amount of PII necessary to facilitate the purpose of reuniting displaced individuals with their families and household members. To mitigate the risk of NEFRLS containing inaccurate information, FEMA collects information directly from the displaced individual. In addition to reduce risks against misuse of NEFRLS information, FEMA uses a third party contractor to authenticate the identity of individuals searching the system to help ensure that only the persons designated by the displaced individual registering in NEFRLS can access or view their information.

Section 2.0 Uses of the Information

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

2.1 Describe all the uses of information.

The information in NEFRLS is used to facilitate the reunification of family and/or household members that have been displaced after a Presidentially-declared disaster or emergency. This includes sharing information that will assist Government agencies, non-government agencies, federal, state, tribal and local law enforcement officials and non-profit organizations such as the Office of Juvenile Justice and Delinquency Prevention, Department of Health and Human Services, U.S. Department of Justice, FBI's Crimes Against Children's Unit, U.S. Department of Justice U.S. Marshals Service, The American Red Cross, and the National Center for Missing and Exploited Children, in reuniting displaced individuals (including medical patients) with their family members (discussed in Section 5.0 of this PIA).

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

NEFRLS uses a commercial data provider for identity verification and authentication of new users (including 'registrants' and 'searchers') registering on the NEFRLS system during disasters. The third party authentication service asks individuals a set of questions and if the individual answers to the satisfaction of the authentication service, the DHS/FEMA will receive a response back as "approved." No other information is being provided back to FEMA from this commercial data provider. Beyond use of the commercial data provider, the system does not analyze or manipulate the data; rather, NEFRLS provides a repository of information that authorized users can search to locate displaced individuals.

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

NEFRLS passes personal information of the registrant or searcher to a commercial data provider for identity verification and authentication purposes. The data sent to the commercial data provider includes first name, last name, date of birth, and address. This data is sent to the commercial data provider to verify that a person with these attributes exists. If information provided by the registrant or searcher is not correct or cannot be verified, then the registrant is provided additional opportunity to provide the necessary

information. If the commercial data provider is able to resolve the identity then four questions are presented to the individual. The individual is given two attempts to answer three out of the four questions correctly to continue with the registration or search process.

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.

FEMA uses NEFRLS information to facilitate the reunification of family and/or household members that have been displaced as a result of a Presidentially-declared disaster or emergency. To ensure uses are consistent with this purpose, NEFRLS employs controls to ensure only authorized individuals may use or search the system. This is accomplished in part through the registration process whereby the displaced individual designates those individuals ('searchers') authorized to view their information. Further, NEFRLS uses a commercial data provider to provide identity verification and authentication for registrants and searchers.

Section 3.0 Retention

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

3.1 What information is retained?

All information identified in section 1.1 of this PIA will be retained in accordance with both NARA and FEMA Record Schedules as documented in this section.

3.2 How long is the information retained?

In accordance with the FEMA Records Schedule (FRS), the National Archives, and Records Administration (NARA) Disposition Authority number N1-311-09-1, records and reports related to and regarding registrations and searchers in NEFRLS performed by a displaced person, Call Center Operator on behalf of a displaced person, or family and friends will be cut off 60 days after the last edit to the record and destroyed/deleted 3 years after the cutoff. Additionally, in compliance with FRS, NARA Disposition Authority number N1-311-04-5, Item 3, records in this system associated with a domestic catastrophic event will have permanent value. A catastrophic event may be any natural or manmade incident, including terrorism, which results in extraordinary levels of mass casualties, damage, or disruption severely affecting the population, infrastructure, environment, economy, national morale, and/or government functions. A catastrophic event could result in sustained national impacts over a prolonged period of time; almost immediately exceeds resources normally available to state, local, tribal, and private-sector authorities in the impacted area; and significantly interrupts governmental operations and emergency services to such an extent that national security could be threatened.

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

A Request for Records Disposition Authority has been submitted to NARA (job number N1-311-09-1) and approval is pending.

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

Risks associated with the length of time data is retained include misuse of data, loss of data, inadvertent release of data, and identity theft. To minimize these risks, and in conjunction with strict access control to the system, NEFRLS will limit its retention of files to 3 years following a disaster. A 3-year retention period mitigates these privacy risks by retaining information only for as long as is relevant and necessary to accomplish the purpose of NEFRLS. FEMA has determined that this retention period appropriately balances evacuees and family members' need to request personal information for documentation purposes against privacy risks.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing information 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 NEFRLS information with internal organizations on a need-to-know basis. For example, FEMA may share information with the DHS Office of Inspector General or any other DHS office in response to a request for information as to why an individual could not locate an evacuee during a disaster.

4.2 How is the information transmitted or disclosed?

Sharing of data internally to authorized personnel is transmitted via email, phone, or hard copy.

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.

There is a risk that information provided to other departments and components within DHS maybe used for purposes other than those discussed within this PIA. To mitigate risks against inappropriate internal sharing, FEMA limits the sharing of PII collected in NEFRLS to internal organizations that demonstrate a need-to-know for the information on an individual case-by-case basis.

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

Evacuee information as identified in section 1.1 of this PIA will only be shared with the following agencies for the purpose of searching for missing persons during a Presidentially-declared disaster:

- Department of Justice (DOJ) Office of Juvenile Justice and Delinquency Prevention (OJJDP);
- Department of Health and Human Services (DHHS);
- U.S. Department of Justice FBI's Crimes Against Children Unit (CACU);
- U.S. Department of Justice U.S. Marshals Service (USMS);
- National Center for Missing and Exploited Children (NCMEC);
- American Red Cross (ARC);
- Federal state, local and tribal law enforcement officials
- National Archives and Records Administration;
- Congressional Office's; and
- Voluntary organizations as defined by 44 CFR § 206.2(a)(27).

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.

The sharing of PII outside of the Department of Homeland Security will be in accord with the original purpose of the collection as stated in DHS/FEMA – REG 2 "Disaster Recovery Assistance Files" SORN "to a Federal or State law enforcement authority, or agency, or other entity authorized to investigate and/or coordinate locating missing children and/or reuniting families." Additionally, sharing of information in the NEFRLS system can be reviewed in the "National Emergency Family Registry and Locator System Files" SORN published in the Federal Register. Also, as required by Section 689c of PKEMRA, FEMA entered into a Memorandum of Understanding (MOU) with the Department of Justice (DOJ), the Department of Health

and Human Services (HHS), the American Red Cross (ARC), and the National Center for Missing and Exploited Children (NCMEC) to facilitate sharing of information for the purpose of re-uniting families. Information from the NEFRLS will be shared with internal and external agencies (via MOU) and law enforcement officials through written request to FEMA authorized NEFRLS System Administrators.

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

The external organizations listed in Section5.1 will be required to submit their request in writing, either electronically through a 128-bit secure system or by paper copy, to the FEMA Disaster Assistance Directorate (DAD) Director or to the individual identified and authorized by the DAD Director. Each request by Law Enforcement personnel will need to include who they are, badge number, what agency and where they are located, the name(s) of the individuals the external organization is requesting information on. The information returned to the requesting entity will include part or all of the information disclosed by the registrant based on its need-to-know. Information will be sent to the requesting entity by paper copy via First Class Mail requiring a signature.

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

There is a risk that information provided to other departments and agencies outside of DHS may be used for purposes other than those discussed within this PIA. To mitigate risks against inappropriate sharing of NEFRLS information outside of DHS, FEMA limits the sharing of personal information collected in the NEFRLS to external agencies on an individual basis. Specifically, FEMA will review each request to determine whether or not it meets the standards for sharing set out by the SORN routine uses. FEMA also mitigates its risks through entering into MOUs with external partners as outlined in Section 5.2. In these and any circumstance where direct "limited" access is granted an MOU/MOA is entered into between FEMA and the respective agency that addresses all Privacy Act compliance, protection, systems security, access and training requirements that the requesting entity must meet first. Training will be provided to FEMA operators at FEMA's Texas National Processing Service Center (NPSC) only.

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, a SORN (see attached) will be published in the Federal Register prior to the system being accessible. In addition, both the displaced individual registering in the system and the individual searching the system will be required to agree to a Privacy Act Statement (see Attachment #1). If they are accessing the system

via the website they will be provided an electronic copy that they will be asked to read and agree by way of a check box. They will have the option of printing the statement for their records if they choose to do so. For those individuals accessing the system through the toll free number, the Privacy Act Statement will be read to them and they will be required to agree to the statement before they will be able to proceed with their registration. Upon the individual's request, a hard copy of the statement will be sent to them.

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

Yes, registration and use of NEFRLS is completely voluntary. An individual registering in the system can delete his/her registration at any time before they complete the registration process. When a registrant selects to delete their registration the information is purged from the database. However, a user cannot delete their registration from the system once they have confirmed and submitted their registration.

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

Yes. Individuals may designate specifically which other individuals may view their personally identifiable information. However, in certain instances as noted in the system of records notices, DHS/FEMA may share the personally identifiable information with federal agencies; state, tribal and local governments; federal, state, and local law enforcement agencies; the National Center for Missing and Exploited Children and voluntary organizations as defined in 44 CFR 206.2(a)(27) that have an established disaster assistance program to address the disaster-related unmet needs of disaster victims, are actively involved in the recovery efforts of the disaster, and either have a national membership, in good standing, with the National Voluntary Organizations Active in Disaster, or are participating in the disaster's Long-Term Recovery Committee for the express purpose of reunifying families.

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

Notice is provided at the point of collection online and displaced individuals registering in the system and individuals searching the system are required to indicate if they have read and accepted the terms of the Privacy Act statement before they can proceed with their registration or search.

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?

The procedure for individuals who have registered with NEFRLS to gain access to their own information is to return to the website or via an operator-assisted toll free number and select to edit their registration. This information is explained on the NEFRLS overview and instruction page. The system authenticates the individual once he/she is identified either by the user's unique user name and password or by completing the third-party identity verification and authorization process. If authenticated, the individual will then be able to access their registration and alter the information they entered. If identity cannot be authenticated after the 2nd attempt, the individual should contact a NEFRLS Human Service Specialist at 1-800-588-9822 for further assistance.

The procedure for individuals to gain access to obtain additional information, such as who has accessed their message or who has provided information, is listed both in FEMA and the DHS Privacy Act regulations, 44 C.F.R. Part 6 and 6 C.F.R. Part 5. Requests for Privacy Act protected information must be made 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 identity must be clearly indicated. Requests should be directed to: FEMA, FOIA/Disclosure Branch, Records Management Division, 500 "C" Street, SW, Washington, D.C. 20472

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

The procedure for correcting erroneous information is identical to the procedures for accessing an individual's own information. The registrant returns to the website or via an operator-assisted toll free number and selects the option to edit his/her registration.

The system provides an information confirmation page before users submit information. This will ensure the user has entered the correct information and helps decrease erroneous entries.

In addition, an individual can correct erroneous information in accordance with both DHS and FEMA Privacy Act regulations as identified in 7.1.

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

The procedure for individuals to amend their information is explained on the NEFRLS overview and instruction page and is accessible both at the time of registration and whenever the individual accesses their account.

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

As indicated above, individuals may gain access to, and request correction of their record.

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

If registrants are not able to access, update or correct their information, the risks of mistaken identity, a registrant's information going to an unauthorized person or an authorized searcher accessing erroneous or out of date information about a registrant is increased. To help reduce these risks, any individual who has registered in NEFRLS may edit their information at any time by calling the 800 number or by using the Internet by selecting the "Edit My Information Page."

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?

Technical, operational, and management controls are in place, allowing authorized users access only to the personal data necessary for each user's official role and his or her required use of data. NEFRLS processors and call center operators are only allowed to modify data as specifically requested by the individual in order to perform their roles.

A detailed description of the technical and management controls regarding identification and authentication, logical access controls, and public access controls is documented as part of the IT Certification and Accreditation Process. Such security documents are not available for broad review for security reasons. Access to data is controlled through use of the identity verification and authentication process and through the use of a unique user ID and password combination. Strong passwords following DHS standard are required by system and application controls. User passwords must be changed on a regular basis. Additionally, secure sockets layer (SSL) encryption is used to protect the transfer of data. The data is hosted in a secure infrastructure with servers protected by controls such as the monitoring of audit logs, management of vulnerabilities, and escalation for any unauthorized data use are in place. The DAD Director will assign gatekeepers/system administrators who will be exclusively tasked with assigning DHS staff with access to the system and roles to users.

8.2 Will Department contractors have access to the system?

Yes, limited user access is described in Section 8.1 above only for contract personnel working on IT and computer support and contracted call center operators/data processors. Contractors, unless specifically cleared, will not have access to the system.

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

These individuals will be registered and authenticated in accordance with the National Institute of Standards and Technology Level 2 Assurance guidelines. Additionally, all FEMA employees and contractors are required to complete FEMA Office of Cyber Security annual Security Awareness Training. All contract employees are required to adhere to the Privacy Act / Confidentiality clauses as per terms of their contracts with FEMA.

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

NEFRLS currently resides in an "Agile System Development" environment for which a completed C&A and Authority to Operate (ATO) was obtained on May 3, 2007. A C&A Lite package was submitted for NEFRLS on March 23, 2007. NEFRLS is currently going through a full C&A in order to move NEFRLS to the production environment and an ATO is in the process of being obtained.

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

The following controls are in place to prevent data misuse:

- Audit trails (activity logs) and reporting capabilities are enabled and secured on the operating systems, applications, and middleware. FEMA conducts periodic reviews of all user access.
- Displaced individuals registering in NEFRLS will have restricted access only to their personal data and only after they have completed the identity verification and authentication process.
- Individuals searching the system will be issued a user name and password after they have completed the identity verification and authorization process and will only be granted restricted, read-only access to the information the registrant has authorized them to view. The user name and password will be effective to access their authorized information for up to 60 days after the last edit date of the registration.
- FEMA employees and contractors will be granted restricted access as outlined in 8.1 above, and are required to have a "Public Trust" or higher clearance as user names and passwords will be managed by the National Emergency Management Information system Access Control System (NACS). NACS is the FEMA standard for secured access control for software applications.
- Computer incident response procedures are established to address and escalate reported security incidents as quickly as possible.
- Procedures for tracking problems will be established to enable users of the NEFRLS system of records to report any observed or suspected security weakness in, or threats to, systems or services and software malfunctions, so that they are addressed quickly.

- Procedures for handling and storage of information will be established to restrict access to unauthorized users.
- A "time-out" feature will drop a user's connection after idle periods to protect against unauthorized users accessing unattended but connected computers.

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

The information collected and stored by NEFRLS, if not appropriately protected, could allow an unauthorized person to assume the identity of another person. Additionally, if unchecked, individuals could locate a person for purpose of criminal activities or for purposes outside of that of reuniting families. FEMA has instituted strong security controls to ensure that the information collected in NEFRLS is protected throughout the process. This includes access controls, audit trails, and encryption. These are described further in detail above in Section 8.5.

Section 9.0 Technology

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

9. 1 What type of project is the program or system?

NEFRLS is an information technology project and is a web-enabled system.

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

The NEFRLS follows the DHS Information Assurance and Infrastructure Protection IT Project Lifecycle. NEFRLS is currently in a Testing Development Lab (TDL) within a FEMA facility currently in stage 6 of 7 within the lifecycle.

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

No. Appropriate security measures are in place to ensure the confidentiality and integrity of Personally Identifiable Information (PII). To identify current and emerging threats and to mitigate any risks associated with the architecture, a risk assessment will be conducted periodically.

Approval Signature

Original signed and on file with the DHS Privacy Office
Mary Ellen Callahan
Acting Chief Privacy Officer
Department of Homeland Security

Appendix (NEFRLS Privacy Act Statement)

National Emergency Family Registry and Locator System (NEFRLS)
Simplified Privacy Act Statement
07/23/08

Authority: The Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act), 42 U.S.C. Sections 5121-5207; Executive Order 12148, as amended cited as;, "Post-Katrina Emergency Management Reform Act of 2006," (PKEMRA) Pub. L. 109-295, in Section 689c authorizes the collection of the information described below.

Purpose: The primary use of this information is to help reunite displaced individuals with their family and household members following a Presidentially declared disaster or emergency under the Stafford Act. Displaced individuals who register (called "registrants") may select up to (7) seven family members and/or household members they want to have access to the "personally identifying information" they have posted. These designated family and/or household members (searchers) may obtain access to the information posted by the registrant if they can verify their identity as an individual authorized to limited access by the registrant.

Routine Uses: In addition to disclosures generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act, all or portions of records contained in this system may be disclosed outside the Department of Homeland Security as a routine use pursuant to 5 U.S.C. § 552a(b)(3) as follows:

(A) Reunification of Families: To Federal agencies; State, tribal and local governments; Federal, State, and local law enforcement agencies; The U.S. Department of Justice, Office of Juvenile Justice and Delinquency Prevention(OJJDP); The Department of Health and Human Services (DHHS); The U.S. Department of Justice, FBI's Crimes Against Children Unit (CACU); The Department of Justice U.S. Marshals Service (USMS); The National Center for Missing and Exploited Children (NCMEC) and voluntary agencies as defined in 44 CFR 206.2(a)(27) that have an established disaster assistance program to address the disaster-related unmet needs of disaster victims, are actively involved in the recovery efforts of the disaster, and either have a national membership, in good standing, with the National Voluntary Organizations Active in Disaster (NVOAD), or are participating in the disaster's Long-Term Recovery Committee for the express purpose of reunifying families. Other agencies may include other Federal agencies and non-governmental agencies with which FEMA coordinates under the National Response Plan and after March 22, 2007, the National Response Framework, which is an integrated "plan" explaining how the Federal Government will interact with and support State, local, tribal, and non-governmental entities during an incident such as a Presidentially-declared major disaster or emergency. This may include: the Office of Juvenile Justice and Delinquency Prevention(OJJDP), FBI's Crimes Against Children's Unit(CACU), DOJ's U.S. Marshals Service(USMS), Department of Justice (DOJ), the Department of Health and Human Services, the American Red Cross, the National Center for Missing and Exploited Children and the National Emergency Child Locator Center.

(B) To a congressional office from the record of an individual registrant (e.g. displaced individual) in response to an inquiry from that congressional office made at the request of the individual to whom the records pertains.

(C) To DOJ or other Federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when: (1) DHS, or (2) any employee of DHS in his/her official capacity, or (3) any employee of DHS in his/her individual capacity where DOJ or DHS has agreed to represent the employee, or (4) the United States or any agency thereof, is a party to the litigation or has

an interest in such litigation.

(D) To the National Archives and Records Administration or other Federal Government agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. sections 2904 and 2906.

(E) To appropriate agencies, entities, and persons when (1) DHS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

(F) To an agency, organization, or individual for the purposes of performing authorized audit or oversight operations.

(G) Where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law – criminal, civil or regulatory – the relevant records may be referred to an appropriate Federal, State, territorial, tribal, local, international, or foreign agency law enforcement authority or other appropriate agency charged with investigating or prosecuting such a violation or enforcing or implementing such law. In the event of circumstances requiring an evacuation, sheltering, or mass relocation, FEMA may also share applicant information with Federal, State or local law enforcement in order to address public safety or security issues.

(H) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records.

Disclosure: In order to verify the identity of the registrant and/or the person searching for the registrant, security precautions have been implemented. Therefore, personally identifying information, including but not limited to, pre-disaster address, phone number and gender will be requested from either the displaced individual registering in this system, or the searcher of the system for a missing family or household member. Registration of your personal information is entirely voluntary, but failure to provide certain information or failure to pass the identity verification and authorization process will prevent an individual from registering in this system and/or prevent an individual from receiving information on a registered individual.

By continuing with the registration process you agree that:

□ I understand that the terms of the Privacy Act of 1974 allows any information submitted into NEFRLS may be subject to disclosure upon written request with agencies and organizations outlined in the Routine Use section of this notice..

□ I am voluntarily entering my "personally identifying" information into the National Emergency Family Registry and Locator System.