Privacy Impact Assessment for the

OMB 90-69 FEMA Form

8-16-2006

Contact Point
George Fraley
TXNPSC
Recovery
940-891-8696

Reviewing Official Maureen Cooney Acting Chief Privacy Officer Department of Homeland Security (571) 227-3813

Abstract

The abstract should be a short paragraph, four sentences or less, that describe:

- The general type of information used.
- What the information is used to accomplish.
- Why it is important to use the information for that accomplishment.

This collection of information is generated by individuals who apply for disaster assistance

APPENDIX B: FEMA Form 90-69

benefits under the Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended. It also complies with the provisions of Title IV of the Personal Responsibility and Work Opportunity Reconciliation Act of 1996, 8 U.S.C. §§1601 et seq.

Introduction

The introduction should contain the following elements, and should not exceed one page:

• The system name, the unique system number if there is one, and the name of the DHS component(s) that own(s) the system;
• The objective of the new program, technology and/or system and how it relates to the component's and DHS's mission;
• A general description of the information in the system and the functions the system performs that are important to the component's and DHS's mission; and
• A general description of the modules and subsystems, where relevant, and their functions. For longer more in depth descriptions, an appendix may also be appropriate.

The Department of Homeland Security (DHS)/Emergency Preparedness and Response (EP& R)'s/Federal Emergency Management Agency (FEMA's) objective of this Privacy Impact Assessment (PIA) is to identify and to address the safeguarding of personal information that may result from collecting data for registrations to federally declared disasters or emergencies. This PIA document reexamines the privacy implications to ensure that adequate privacy considerations and protections have been applied.

The NEMIS (National Emergency Management Information System) IA (Individual Assistance) Module is where FEMA collects this data and stores it in the NEMIS system for assistance eligibility processing. The information is for OMB 1660-0002 approval of the registration forms in English and Spanish and the Declaration and release forms in English and Spanish.

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?

Personal information pertaining to individuals applying for Federal Assistance including: an individual's name, home address, Social Security number, home phone number, temporary address and phone numbers, personal financial information including applicant's bank name, bank account information, insurance information, individual or household income, the home's number of occupants, and the dollar amount of their disaster losses. See Appendix A OMB 90-69 FEMA form.

1.2 From whom is information collected?

Information is collected directly from individuals applying for a Federally declared disaster by phone, over the Internet, or in person completing the OMB 90-69 FEMA

- Total number of vehicles for the household that are drivable. Insert number.

Field 26.

- IN TABLE: List the type of insurance that the applicant held at the time of the disaster, including but not limited to sewer backup, earthquake, real property, and/or personal property. Include the name of the insurance company.

Field 27.

- IN TABLE: List information for the applicant and all other persons/dependents, whether or not they are related to the applicant, who considered the home to be their primary residence at the time of the disaster. It is important that the applicant's SSN be included.

Field 28.

- Self-employed as a Primary Source of Income: YES/NO
- Primary Source of Income: insert information
- Number of claimed dependents: insert information.
- Combined individual or household pre-disaster gross Income: insert information. Check box: (weekly, bi-weekly, monthly, quarterly, or yearly).

Field 29.

- Electronic Funds Transfer: YES/NO
- Institution name: enter information
- Routing No.: enter information (9 digit number)
- Account type by marking the Checking or Savings box.
- Account no.: enter information.

Field 30.

- Enter any additional comments as necessary.

Form.

1.3 Why is the information being collected?

Information is collected to fulfill the mandates of the Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended and provide eligible victims with disaster assistance for which they qualify. This collection greatly reduces the paperwork burden to applicants so they are not contacting multiple agencies for assistance.

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

The legal basis for collection of information in support of the applicant as well as administrative policy is contained in the Robert T. Stafford Disaster Relief and Emergency Assistance Act, Public Law 93-288, as amended; and 44 Code of Federal Regulations. It also complies with the provisions of Title IV of the Personal Responsibility and Work Opportunity Reconciliation Act of 1996, 8 U.S.C. §§1601 et seq.

Homeland Security

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.

The Department of Homeland Security's Privacy Office has made protecting the privacy of ordinary citizens a top priority. The NEMIS (National Emergency Management Information System) IA (Individual Assistance) Module is in full compliance with this priority. FEMA collects this data and stores it in the NEMIS system for assistance eligibility processing. Applications are taken over the phone by a FEMA representative or on the Internet using a 128-bit encrypted secure Internet connection.

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.

- Check Unknown if the applicant does not know if the home is damaged or unsafe.

Field 13a.

- Primary Residence

Field 13b.

- Own or Rent: check box selection

Field 13c

- Residence type: check box selection but allows for Other selection w/ comment

Field 14.

- Personal Property Damage: YES/NO

Field 15.

- Utilities out: YES/NO

Field 16.

- Inaccessible Due to the Disaster: YES/NO

Field 17.

- Inaccessible due to mandatory Evacuation: YES/NO

Field 18.

- Lost time at work: YES/NO

Field 19.

- Medical, Medical Personal Property, and/or Dental Expense: YES/NO
- Insurance Coverage: YES/NO
- Insurance company name.
- Amount.

Field 20.

- Moving/Storage: YES/NO
- Insurance Coverage: YES/NO
- Insurance Company.
- Amount.

Field 21.

- Other Expenses: YES/NO

Field 22.

- Funeral Expense: YES/NO

Field 23.

- Business Affected: YES/NO
- Business name.
- Business Related Essential Tool/Equipment: YES/NO
- Does your business operate as a Private not-for-Profit Org.?: YES/NO

Field 24.

- Farm or Ranch Damage: YES/NO

Field 25.

- Total number of vehicles for the household. (year, make, and model). Insert information.
- Vehicles Damaged: YES/NO
- Provide information IN TABLE: Comprehensive and/or Liability Insurance, and if the vehicle(s) is registered.

The information collected from individuals enables FEMA to record losses suffered from disasters and emergencies in order to assist eligible applicants. This information is also used to prevent the duplication of disaster benefits provided by FEMA, Federal and state and local disaster agencies.

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

No.

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

The applicant is given an opportunity to review their information at the end of the application process. Applicants also receive a copy of their completed application in the mail.

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.

The information collected is subjected to a set of automated business rules for the purpose of ensuring that victims in a disaster are handled in a standard and equitable manner. The business rule set is reviewed frequently and managed by the program office. NEMIS, as a major mission-critical FEMA application, is subject to continuous monitoring, testing, and evaluation in the course of certification and accreditation, system releases, system acceptance testing, and audits by the DHS Office of the Inspector General and various FEMA program offices that are dependent upon NEMIS for mission support services. Agents who access case files, on behalf of callers to the 800#, verify the identity of applicants before discussing details of the case. The internet controls access to applicant data according to national information systems and technology standards level two which requires user generated pin and passwords for access.

APPENDIX A

DATA ELEMENTS

Application/Registration for Disaster Assistance

FEMA Form 90-69

Field 1.

- Selection of prefix or title, such as Mr. or Ms.
- Last name, first name, and middle initial of the applicant.
- Name suffix such as, Jr., Sr., etc.

Field 1.a.

- Language Spoken by the applicant.

Field 2.

- Applicant's social security number (SSN).

Field 3.

- Full physical street address at which the damage occurred.

Field 4.

- Date the damage occurred.

Field 5.

- Phone number used in the applicant's home at the time of the disaster.
- Second phone number that was in the home at the time of the disaster.

Field 6.

- Current Phone No.

Field 7.

- Applicant's e-mail address.

Field 8.

- Cause of Damage to the home

Field 9.

- Current Location where the applicant is living.

Field 10.

- Applicant's mailing address.

Field 11.

- If the applicant's current mailing address is not located in the U.S. or one of its territorial possessions (e.g., Puerto Rico, Virgin Islands, Guam), please enter the full Foreign Address.

Field 12.

- If the applicant has Essential Needs YES/NO

Field 13.

- If the applicant has damage to the home (e.g., electrical, heating, floors, walls, ceilings, and foundation), check Yes.
- If the applicant's home is unsafe, check Yes.

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 data in the system are considered federal government records. The records retention period for this data is 6 years and 3 months from the close of the case.

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

The retention periods for data are consistent with retention schedules established by the National Archives and Records Administration (NARA).

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

The data are retained consistent with NARA retention schedules. According to the NARA, record schedules are used to ensure that data are: organized and maintained in such a way as to be easily retrieved and identifiable as evidence of the program's activities, especially in the event of an audit, a Freedom of Information Act (FOIA) request, or a discovery in a lawsuit; conserves space; saves money; and helps preserve the records that are valuable for historical or other research purposes.

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?

The DHS Office of the Inspector General (OIG) may request access to the data.

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

The OIG is responsible for the audit of agency programs and operations, including fraudulent applications for Presidentially declared disaster assistance.

4.3 How is the information transmitted or disclosed?

3 PRIVACY IMPACT ANALYSIS

DHS guidelines and Federal Law require a PIA when:

- Creating any new collection of personal information
- Employing, developing and/or procuring any new technology or system that can store and thus reveal a person's identity
- Creating new database(s) or view(s) from old databases or systems

This privacy impact assessment was conducted because this major system enhancement adds a new method of collecting the existing personal information data elements (electronically via the Internet) that may pose some privacy concerns.
The detailed privacy impact assessments are provided in Part A.

The OIG may be given access to the data as requested in order to perform their responsibilities related to investigation of fraud or they may request a report of applicant data. Data reports are delivered to local OIG as a print out or sent via secure electronic transmission.

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

No critical vulnerabilities were identified.

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?

US Treasury
SBA
States Other Needs Program

5.2 What information is shared and for what purpose?

Treasury uses name, bank account, and address information from the registration to issue payments to eligible applicants.

The Small Business Administration (SBA) provides loan assistance to applicants who may not be eligible for Individual Assistance from FEMA.

State's Other Needs Assistance Program Offices have information based on income, insurance, and need, in disasters where the state has opted to direct their own Other Needs Assistance Program.

5.3 How is the information transmitted or disclosed?

The information is processed through secure systems interfaces specific to each agreement to ensure that each agency can access only the information necessary for their mission.

5.4 Is a Memorandum of Understanding (MOU), contract,

107 and the President's Government to Citizens Initiative as discussed at www.whitehouse.gov/omb/egov/pres_initiatives.htm.

When the information is processed, the individual's record is automatically updated to reflect the status of their specific application. Applicants may call to check on the status of their application, and the individual may also call in updates to the personal information on their application. It is especially important to maintain up-to-date information on the applicant that will speed up the application processing and render assistance quickly and equitably. These limited updates include an individual's temporary address and phone number, social security number, and bank routing and account numbers for electronic funds transfers, where appropriate. Accordingly, we are proposing to add a corresponding Internet capability that will provide applicants the ability to inquire about the status of their own applications only, and to update only their limited personal data electronically.

2.3 Information Type

Under the currently existing Privacy Act system of records, the FEMA IA Program staff collects the following types of privacy information in order to identify the individual applying for disaster assistance: an individual's name, home address, Social Security number, home phone number, temporary address and phone numbers, personal financial information including applicant's bank name, bank account information, insurance information, individual or household income, the home's number of occupants, and the dollar amount of their disaster losses. A detailed description of each element and a copy of the FEMA Form 90-69 from which the information is extracted is provided in Appendix A.

Depending on the nature of the disaster/emergency and subsequent losses, individuals may be referred to other Federal, state or local agencies and organizations authorized to provide disaster assistance, such as the Small Business Administration, the American Red Cross, the Internal Revenue Service, etc. The applicant is informed when FEMA initially collects their personal information collection about the Privacy Act and the possible sharing of their information with these referral agencies. The sharing proceeds pursuant to one of the routine uses published in the existing system of records, Disaster Recovery Assistance Files, which will published very shortly in the Federal Register.

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?

Signed Memoranda of Understanding and Interface Security Agreements govern the use of the data by other agencies. FEMA's Office of the Chief Financial Officer signs agreements with Treasury. The Chief Information Officer (CIO) of each agency signs the Memorandum of Understanding between FEMA and SBA.

5.5 How is the shared information secured by the recipient?

The required information is documented in the Agreements described above between the Federal agencies and FEMA. The information is processed through documented systems interfaces specific to each agreement to ensure that each agency can access only the information necessary for their mission.

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

Such information would be documented in the MOU Agreements described above between the Federal Agencies and FEMA.

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

No critical vulnerabilities were identified. All information related to the external sharing would be documented in the MOU Agreements described above between the Federal Agencies and FEMA.

Homeland Security

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

2 AGENCY PROCESS

The Department of Homeland Security's Privacy Office has made protecting the privacy of ordinary citizens a top priority. The NEMIS IA Module is in full compliance with this priority.

2.1 System Description

NEMIS is an enterprise-wide automated system that integrates hardware, software, telecommunications, applications software, and operational procedures to handle the processing and management of disaster victim assistance to individual citizens and public assistance to State and local government entities. FEMA works closely with the Small Business Administration (SBA), and may share selected data with the SBA. Formalized agreements are in place with SBA for the information sharing to be limited to "official use" only for FEMA and SBA purposes. State governments are granted limited access to data from only its State's citizens. In both cases, access to the data is limited and controlled. Only authorized FEMA officials have access to the composite data source.

Data submitted via the Internet are input via a 128-bit Secure Socket Layer (SSL) Internet connection. The disaster victim, who supplies the data originally, may access only their own personal data and no other applicant's. The disaster victim authenticates their own information at the time of submission of their own data. Each individual is granted only limited access through a user id, password, and personal identification number (PIN) supplied by FEMA, in order to gain subsequent access only to their own data. Access to the data is granted in accordance with National Institute for Standards and Technology (NIST) Level 2 Assurance Level. Exposure of the data via the Internet is highly restricted and controlled in several layers to protect the data. No user accounts on the Internet are permitted direct access to the NEMIS database. The user's request for his specific record passes through three firewalls and the request is serviced by a trusted account behind the third firewall. The single record results are then passed back to the user, thus protecting the database. Each firewall serves to prevent unauthorized intruders from gaining access to systems behind that firewall. FEMA has implemented a series of these protection zones, which require successive penetration of each firewall to gain access to the subsequent one unless an authorized account is used.

2.2 Reason for Collecting Privacy Data

The collection of such personal information is necessary for FEMA to carry out its mission of assisting individuals who apply for disaster assistance benefits under the Robert T. Stafford Disaster Relief and Emergency Assistance Act. Complete legal descriptions are provided in Appendix B.

The Internet-based data collections provide disaster victims an alternate means of submitting their requests for disaster assistance, (e.g. electronically) especially when the phone teleregistration process is unavailable due to high demand after a disaster. This method of delivery of service is strongly endorsed and supported by the Public Law 106-

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?

Applying for disaster assistance is voluntary. Applying constitutes consent to the collection of this information. A Privacy Act statement is presented to the applicant upon entering the Internet site that informs the registrant with whom this information may be shared. Through this electronic method, the registrants are required to check a box that indicates that they have read the Privacy Act notice presented and agree to it's provisions. This same Privacy Act Statement is read to those registering via the telephone. See Appendix B for Privacy Act Statement.

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

Individuals always have the right not to apply for Federal disaster assistance. In addition, registrants have the opportunity at any stage of the registration process to decline to provide basic identifying information and, thus to withdraw their application. However, individuals are informed that in order to process their request for assistance, registrants must provide all required information.

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?

Applying for disaster assistance constitutes consent to the collection of this information. The information provided is only used to provide disaster assistance and to prevent duplication of benefits in accordance with the routine uses listed under the existing Privacy Act system of records, the "Disaster Recovery Assistance Files".

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

No critical vulnerabilities were identified.

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

1.2 Scope

We propose to make the Internet available for individuals to apply for disaster assistance in addition to the paper FEMA Form 90-69 application, and calling in through the telephone interview method. The proposed upgrade to the existing NEMIS IA Module would allow disaster victims an additional method to apply (electronically through accessing the Internet) for Individual Assistance (IA) disaster assistance. The new electronic method of applying for disaster assistance is the reason for this Privacy Impact Assessment (PIA). The Internet process will collect the same information that is currently collected by the paper and the telephone interview process under the existing Privacy Act system of records. Once collected, the Internet-supplied information from the individual will be processed and protected in the same manner with the same electronic safeguards in NEMIS, as the information transcribed from the paper form , or entered during the telephone interview method. In effect, the FEMA Form 90-69, "Disaster Assistance Registration/Application" form will be accessible electronically over the Internet at FEMA's website via a 128-bit secure connection. The FEMA web site will be advertised on //WWW.FEMA.GOV.

A description of the specific types of personal data to be collected on the FEMA Form 90-69 is itemized within Appendix A.

This PIA describes the IA programs and the NEMIS system's processes for protecting the privacy of personal information collected for disaster assistance in accordance with the Department of Homeland Security (DHS) Privacy Office's policy on the electronic collection of personal information. This PIA is intended to:

- Determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an Internet-capable electronic information system, and
- Evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

to gain access to their own information?

A copy of the completed application, OMB 90-69 FEMA Form, is mailed to the applicant, once the application is entered in the NEMIS Registration Intake Module. Additionally, at the time of inspection, the applicant is asked to sign the application and the Privacy Act Statement. Individuals may contact FEMA via published disaster assistance help lines to request information about their application at any time.

7.2 What are the procedures for correcting erroneous information?

There are several ways an applicant can correct erroneous information. The first method is for the applicant to call the FEMA IA Helpline and have the attendant make the necessary corrections. The second is to provide the disaster housing inspector with corrections. The field inspectors have a limited capability to make corrections to erroneous information; consequently, most corrections are best done via the FEMA IA Helpline. A third method to electronically access and update a few key fields of their own record (PIN) assigned to them by FEMA via the Internet. For this method, NIST 800-37 Level 2 Assurance tokens will be required to ensure protection of the data.

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

Information is provided at the time of registration.

7.4 If no redress is provided, are alternatives are available?

Not Applicable.

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.

Applicants are provided with a Privacy Act Statement and application is voluntary. Applicants are able to correct their information.

Section 8.0 Technical Access and Security

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

- Computer Fraud and Abuse Act of 1986, public law 99-474, 18 USC §1030
- Presidential Decision Directive: Critical Infrastructure Protection (PDD-63)
- Executive Order 13010 Critical Infrastructure Protection
- Office of Management and Budget OMB Circular A-123, Management Accountability and Control

- OMB Circular A-127, Financial Management Systems
- OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Information Resources
- National Information Standard Technology (NIST) Special Publications (SP) 800-18, Guide for Developing Security Plans for Information Technology Systems
- NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems
- NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems
- NIST SP 800-30, Risk Management Guide
- NIST SP 800-34, Contingency Planning for IT Systems

In accordance with our existing Privacy Act system of records, the "Disaster Recovery Assistance Files", (66 FR 51436--October 9, 2001), FEMA collects this personal information through applications in one of two ways. 1) Through applications in hard copy (paper) form when an individual fills out a paper application, or 2) by the telephone interview method, by which an individual calls FEMA through a published disaster assistance phone number, and a teleregistrar reads all of the questions, and inputs the individual's answers directly into NEMIS.

In accordance with our existing Privacy Act system of records, FEMA collects this information in hard copy (paper) form, and stores it electronically in the NEMIS system. Specifically, the information has been collected from individuals either through applications in paper form by an individual filling out an application (which is input into the system by FEMA's data entry staff), or via telephone interviews with disaster victims who call in to a published disaster assistance number where FEMA employees record their personal application information directly into the NEMIS system. In either case, the same type of personal information goes into the already existing Privacy Act system of records (the "Disaster Recovery Assistance Files") to be processed by the system. The system used to store and process these data is the National Emergency Management Information System (NEMIS) Individual Assistance (IA) Module. In the telephone interview process, NEMIS provides the teleregistrars with the exact questions to be read to the applicant. The teleregistrar then enters the applicant's verbal response into the corresponding entry on the form. This proposed modification to the NEMIS IA module will use the same tools and processes except that the question will be displayed to the applicant electronically, via the Internet rather than being read to the applicant by a teleregistrar. The applicant will then enter the information into the system via the Internet. A 128-bit encrypted secure Internet connection will be used.

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

FEMA employees and FEMA contractors who pass DHS background checks will have access to perform data-based actions in accordance with their authorized role for official purposes only. Authorized information technology (IT) professionals that handle the operations and maintenance of the system will have limited access to the system to support trouble shooting of technical systems issues encountered on a day-to-day basis. Developers do not have access to the system except as authorized and approved on an individual case-by-case basis for troubleshooting purposes only.

8.2 Will contractors to DHS have access to the system? If so, please submit a copy of the contract describing their role to the Privacy Office with this PIA.

Authorized disaster housing inspection contractors have access to the information collected in order to further assist the applicants for official purposes only.

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

Yes, all internal users are assigned official role-based access based appropriate for their official position in FEMA.

Internet users do not have access to the entire database, only limited access to their own information in an environment controlled by cyber security protocols.

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

Access is managed via automated role-based access controls for official use only. It is restricted by the official roles assigned to that user by virtue of the person's organizational position within FEMA.

Access by applicants depends on FEMA assigning a properly authenticated user id, password, and PIN. No individual will have access to the entire database via the Internet. Applicants will be registered and authenticated in accordance with NIST Level 2 Assurance guidelines.

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

Each position and all roles assigned to the position as well as the definition of each role is documented, managed, and an audit trail is maintained in the automated access control

1 INTRODUCTION

The Department of Homeland Security (DHS)/Emergency Preparedness and Response (EP& R)'s/Federal Emergency Management Agency (FEMA's) objective of this Privacy Impact Assessment (PIA) is to identify and to address the safeguarding of personal information that may result from our proposed addition of an electronic method (via the Internet) of data collection of disaster assistance applications from individuals. This electronic (Internet) method of collecting individuals' personal information on the Federal Emergency Management Agency (FEMA) Form 90-69 will not alter the data elements currently covered by the existing approved system of records (e.g. paper applications). This PIA document reexamines the privacy implications to ensure that adequate privacy considerations and protections have been applied to this electronic framework.

1.1 Background

Rapid advancements in computer technology make it possible to store, retrieve, and associate vast amounts of data quickly and efficiently. These advancements have raised concerns about the impact of large computerized information systems on the privacy of individuals who submit their personal data. Public concerns about highly integrated information systems operated by the government make it imperative to commit to a positive and aggressive approach to protecting individual privacy. Further, there are legal requirements to address these issues as derived from the following references:

- Privacy Act of 1974, as amended, 5 U.S.C. 552a (the "Privacy Act"), Public Law 93-579;
- Computer Security Act of 1987, Public Law 100-235, 40 USC §759;
- Clinger-Cohen Act of 1996, Public Law 104-106;
- Paperwork Reduction Act of 1995, 44 U.S.C. 3501, et seq., as amended;
- Freedom of Information Act, 5 U.S.C. 552 (2000);
- Office of Management and Budget (OMB) Circulars A-130: Management of Federal Information Resources (1996)
- Office of Management and Budget (OMB) Circulars A-123: Management Accountability and Control (1995).

In order to provide assistance to victims of a disaster, the DHS/EP& R/FEMA must collect, store, and manage detailed data on individuals, which is subject to privacy protections in accordance with the foregoing references.
In addition to the foregoing privacy-related documents, FEMA's National Emergency Management Information System (NEMIS), which hosts this system of records, complies with the following guidelines to protect the data stored in the NEMIS databases from unauthorized access:

- Federal Information Security Management Act (FISMA) Title III of the E-Government Act Public Law 107-347
- Government Paperwork Elimination Act (GPEA) Sec 1702

system.

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

The individual applicants are granted only limited electronic access via the Internet. They only have access to their own information, not to the entire database. The individual applicant's access is controlled by NIST Level 2 Tokens.

For users who must process and administer the data in the system, a complete security and access control system is in place which complies with DHS Security guidelines and which includes automatic revocation of access upon expiration of privileges, role-based access controls that prevent browsing, etc.

A time-out feature will drop the connection after a designated idle period to protect against users leaving their computer unattended for extended periods of time.

Managers are responsible for removing access to their respective systems when an individual leaves employment with FEMA.

Access to the system is role-based; therefore, FEMA users have access only to the portion of the data required to perform their official duties.

FEMA Enterprise Operations and the DHS or FEMA Office of Cyber Security are able to monitor system use and determine whether information integrity has been compromised and whether corrective action by the Office of the CIO is necessary. Procedures are compliant with Title III of the E-Government Act of 2000 (Federal Information Security Management Act).

Because unauthorized attempts to upload information or change information are prohibited and may be punishable under the Computer Fraud and Abuse Act of 1986, and the National Information Infrastructure Protection Act, FEMA employs software programs that monitor host and network traffic to identify unauthorized attempts to upload or change information or otherwise cause damage.

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

Internal users are required to complete annual computer security training.

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

The Agency procedures are consistent with the requirements of the Federal Information Security Management Act (FISMA).

TABLE OF CONTENTS

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

FEMA has conducted a risk assessment and no critical vulnerabilities have been identified. Procedures are consistent with FISMA requirements and password protection policies are in accordance with NIST guidelines.

Homeland Security

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 baseline system has been operational since 1997 and was built from the ground up.

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

Security and privacy requirements have always driven the NEMIS (National Emergency Management Information System) architecture, applications, and operations.

9.3 What design choices were made to enhance privacy?

The system can only be accessed from within the FEMA Intranet or via the Internet according to NIST standards level 2 access.

Conclusion

The concluding section should inform the reader, in summary fashion, how you constructed your system, program, rule, or technology based on privacy risks and mitigation strategies.

FEMA is responsible for registering federally declared disaster victims based on the Robert T. Stafford Disaster Relief and Emergency Assistance Act. In order to accomplish this responsibility, FEMA has to collect personal and financial information from disaster victims to

Federal Emergency Management Agency

Submitted by
William S. Prusch
Chief, System Engineering and Development Branch
Information Technology Services Division
Federal Emergency Management Agency

process for assistance eligibility. FEMA also has a responsibility to maintain the privacy of this data. This is accomplished by: presenting a Privacy Act Statement telling applicants how the data will be used, maintaining secure systems with firewalls and NIST Level 2 Assurance, and having role-based access to only allow access as required to perform a specific "official use" function.

Homeland Security

Responsible Officials

<< ADD Privacy Officer/Project Manager>> Department of Homeland Security

Approval Signature Page

_____ <<Sign Date>>

Maureen Cooney
Acting Chief Privacy Officer
Department of Homeland Security