
**Privacy Impact Assessment**
**For**
**The EP&R/FEMA Privacy Act**
**"Disaster Recovery Assistance Files"**
**System of Records**

This Privacy Impact Assessment (PIA) is divided into two parts to facilitate Review. Part A is done in the DHS standard format. Part B provides supplemental background and process information pursuant to this Privacy Impact Assessment within the context of the National Emergency Management Information System (NEMIS) Individual Assistance (IA) module for the Internet.

# Part A: Disaster Recovery Assistance Files

# Privacy Impact AssessmentPRIVACY IMPACT ASSESSMENT
## Information Collections Employing Electronic Capabilities

**Date of Assessment: September 17, 2004**
**FY:2004**

**Information Collection Control Number: OMB 1660-0002**

**Title: Individual Assistance Automation Methods**

**Is this information collection doing any of the following? (PLEASE MARK ALL THAT APPLY)**

**_____ A. Creating any new collection of personal information?**

**__X__ B. Employing, developing, and/or procuring any new technology or system that can store and thus reveal a person's identity?**

**_____ C. Creating new database(s) or view(s) from old databases or systems?**

## SECTION 1. QUESTIONS ABOUT THE DATA AND ITS PURPOSES

**1.1 What information is to be collected?** *(Provide a description of the information being sought from respondents. Specify whether the information is collected directly from individuals, organizations, or local/state/federal governments, and the nature of its content, i.e. personal, financial.)*

**Please see the attached document for all of the specifics that address each of the PIA's questions.***

The information collected is identified in Appendix A of this document. This information is collected directly from the individual and may be both personal and financial in nature.

**1.2 Why is the information being collected? Is it relevant and necessary to the purpose for which the system is being designed?**

*(Provide the statutory citation or regulation that authorizes this information collection, i.e. Public Law # and Section)*

This is a proposed modification of an already existing system of records covered by the provisions of the Privacy Act, the "Disaster Recovery Assistance Files" (66 FR 195, October 9, 2001). The need for this information collection is pursuant to FEMA's mission to provide assistance to disaster victims of Presidentially declared disasters. The legal basis and authorization are: the Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended by Public Law 106-390, October 30, 2000; United States Code Title 42. The Public Health And Welfare Chapter 68. Disaster Relief [As amended by Pub. L. 103-181, Pub. L. 103-337, and Pub. L. 106-390; Pub. L. 106-390, October 30, 2000, 114 Stat. 1552 - 1575); The Robert T. Stafford Disaster Relief and Emergency Assistance Act P.L. 93-288 (42 U.S.C. 5121-5206), as amended and 44 Code of Federal Regulations (44 CFR) Subchapter D--Disaster Assistance, Part 206--Federal Disaster Assistance for Disasters Declared on or After November 23, 1988, the Disaster Mitigation Act of 2000.

In addition, it 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., which governs eligibility for disaster assistance for applicants who are not U.S. citizens.

**1.3 What is the intended use of the information?** *(Specify if the information will be used as a qualifier [i.e. benefits, admissions],*

The information collected from individuals enables FEMA to record losses suffered from disasters and emergencies, and to determine whether an applicant is eligible for assistance. This information is also relevant to prevent the duplication of disaster benefits among FEMA, Federal and state and local disaster agencies, and to provide an understanding of the makeup of a household unit. 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.

**1.4 What are the sources of the information?** *(Specify where and how are you acquiring the information)*

The disaster victims submit their own personal information to FEMA. The disaster victims will register with FEMA in one of three ways: paper, interviewed by a call center teleregistrars who record

callers' information in the NEMIS system; and the proposed method, which is the subject of this PIA, of allowing applicants to self-register electronically via the Internet, and enter their information directly in the NEMIS system via a secure point-to-point secure socket layer tunnel through the Internet. In each method (paper, call center, or self-service via the Internet), the same information will be collected.

FEMA call center staff now provide processing status and make updates to individual applications in response to applicant call-in requests. It is proposed that Applicants, who have previously registered, been authenticated, and given a user identification, password, and personal identification number, be given access to the same status information and be permitted to make the same updates to their applications in the NEMIS via a secure point-to-point secure socket layer tunnel through the Internet. This proposal would enable an authorized disaster assistance applicant to have the ability to access limited information and to update their application electronically.

**1.4.1 Data Collection Instrument(s)** *(Specify, form(s) #, questionnaires, etc.)*

The FEMA Form 90-69, "Disaster Assistance Registration/Application" is the basis of the data collection. The OMB Control Number is 1660-0002. This form is included in Part B of this PIA submission.

**1.5 How will the information be checked for accuracy?**

The applicant is given an opportunity to review their information at the end of the application process. Where appropriate, the applicant is provided with a list of possible answers from which to choose. In addition, the applicant is provided with help text for every requested input field. Applicants receive a copy of their completed application in the mail.

**1.6 Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?**

Not applicable.

**1.7 Will the newly derived data be placed on the individual's record?**

Not applicable.

**1.8 Can the system make new determinations about an individual that would not be possible without the new data?**

No.

**1.9 How will the newly derived data be verified for relevance and accuracy?**

Not applicable, the system does not derive any new data.

**1.10 Are the data elements described in detail and documented? If yes, what is the name of the document?**

Yes, the FEMA Form 90-69, "Disaster Assistance Registration/Application" is the basis for the data. The OMB Control Number is 1660-0002. Appendix A contains a list of the application data elements.

## SECTION 2: QUESTIONS ABOUT REDRESS

**2.1 What opportunities do respondents have to decline to provide information?**

Individuals may choose not to use the Internet method of data submission. However, regardless of the method, certain information is required in order to determine eligibility.

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 for assistance. However, individuals are informed that in order to process their request for disaster assistance, to ensure that the agency complies with applicable laws and regulations, and that no duplication of benefits occurs with other Federal and state organizations or insurance providers, registrants must provide all required information. Further, the individuals may at any time contact FEMA regarding information on their application. All decisions are made based on data in the individual's record, and are communicated to the individual via written correspondence.

**2.2 What opportunities do respondents have to consent to particular uses of the information?**

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."

**2.3 How do individuals grant consent concerning how their information will be used or shared?**

The submission of an application is voluntary. 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 in accordance to the routine uses of the existing system of records identified above in 2.2. Through this electronic method, the registrants are also required to check a box that indicates that they have read the Privacy Act notice presented by the system and agree to its provisions. This same Privacy Act Statement is read to those registering via the telephone or is displayed on the paper application, which the applicant signs and dates.

**2.4 What are the procedures for individuals to gain access to their own information, if applicable?**

A copy of the completed application, FEMA Form 90-69, is mailed to the applicant, once the application is entered in the NEMIS IA 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.

In addition, an individual may contact FEMA's Privacy Officer with questions or concerns.

Rena Y. Kim, Privacy Act Officer, room 840, 500 C Street, SW, Washington, DC 20472; telephone (202) 646-3949.

**2.5 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.

We propose to add a third method to allow the applicant electronically to access and update a few key fields of their own record (PIN) assigned to them by FEMA via the Internet. In implementing this method, NIST 800-37 Level 2 Assurance tokens will be required to ensure protection of the data.

In addition, the individual can also contact the FEMA Privacy Officer.

## SECTION 3: QUESTIONS ABOUT ACCESS TO THE DATA

### 3.1 Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others) and is it documented?

Applicants will have access to all of the data they provide for their own application through the printed Form 90-69 that is mailed to them. Through this electronic module, we propose to give the applicant access to their own information (such as the status of required documentation, inspection status, or SBA status) via the Internet using the Applicant Inquiry/Applicant Update application after FEMA assigns them limited access by password and a PIN.

All access to the personal information/data is managed via a role-based access control system to ensure that only authorized FEMA employees have access to the data for "official use" only. Authorized users are unchanged by our proposal to add the electronic access/Internet method of collecting personal information from disaster applicants. A more in-depth discussion is provided in Part B of this PIA submission.

FEMA employees and FEMA contractors 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 system 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.

Where appropriate, applicants are referred to other Federal agencies such as the Small Business Administration (SBA) for

disaster loan processing. The DHS Office of the Inspector General may request and be given access to the data.

FEMA's authorized Individual Assistance program staff and authorized disaster housing inspection contractors have access to the information collected in order to further assist the applicants for official purposes only.

In addition, certain new "routine uses" in the Amendment will be added to the existing Privacy Act system of records that will further specify who will have access to this information. The proposed "routine uses" include:

1) Information sharing with voluntary agencies active in current disasters; 2) Requests for payment to the U.S. Department of Treasury pursuant to the Debt Collection Improvement Act of 1996, 31 U.S.C. Section 3325(d) and 7701c(1); 3) Billing states for the applicable non-Federal cost share under the Individuals and Households Program; 4) With FEMA contractors who provide support services for the Individuals Assistance (IA) Program; and 5) Emergency evacuation plans of FEMA's manufactured housing units' occupants.

**3.2 How will access to the data by a user be determined?**

Applicants will have limited access to their own information, which they have submitted via the Internet, and to the status of their own information (e.g. the status of required documentation, inspection status, or SBA status) regarding the processing of their own application. Access depends on FEMA assigning applicants a properly authenticated user id, password, and PIN. No individual applying for disaster assistance will have access to the entire database via the Internet.

Applicants will be registered and authenticated in accordance with NIST Level 2 Assurance guidelines. With the exception of Database Administrators, all other FEMA user access is managed via automated role-based access controls for official use only. The user's access into the system is restricted by the official roles assigned to that user by virtue of his or her organizational position within FEMA.

**3.3 Are criteria, procedures, controls, and responsibilities regarding access documented?**

Yes, 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 system.

**3.4 Will users have role-based access to data on the system limiting them to some but not all of the data?**

Yes, all internal users are assigned official role-based access based on their official position in FEMA. The role-based assignment is enforced through automation based on each FEMA employee's organizational responsibilities. As already stated, Internet users (applicants) are not granted access to the entire database, only limited access to their own information in an environment controlled by three firewalls.

**3.5 What controls are in place to prevent the misuse (e.g. browsing, expired privileges, etc.) of data by those having access?**

1. As already stated, the individual applicants are granted only limited electronic access via the Internet only to their own information. Internet users are not granted access to the entire Individual Assistance database. The individual applicant's limited access is controlled by three firewalls. The applicant must use the NIST Level 2 Tokens to gain access to his/her record.
2. For users who must process and administer the data in the system (e.g. FEMA employees and authorized contractors), 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.

3. 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.

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

5. 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.

6. NIST Security Guidelines are followed.

7. 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).

8. 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.

**3.6 Do other systems share data or have access to data in this system? If yes, explain. Include a discussion of who will be responsible for protecting the privacy rights of individuals affected by the interface?**

Yes, the applicant's name, address, and bank account information is sent to the U.S. Department of Treasury, which issues payments to eligible applicants.

FEMA and the States are partners in the provision of individual disaster assistance. Since the Disaster Mitigation Act of 2000, FEMA serves as an agent of most States in providing for "Other Needs Assistance." In cases where the State chooses to process "Other Needs Assistance", selected applicant information is provided to them. In each case, a well-defined approval process is established. A state is granted only limited access; that is, a state can only access its residents' information.

The Small Business Administration (SBA) provides loan assistance to applicants who may not be eligible for Individual Assistance from FEMA. SBA's Disaster Loan Management System accesses NEMIS to check for the duplication of benefits. FEMA has signed a Memorandum of Understanding and an Interface Security

Agreement with SBA to ensure that it protects the privacy and the integrity of applicant's data. The SBA is granted limited access only to the information necessary to administer their program.

**3.7 Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?**

No. Only limited sharing of selected data is provided to the SBA and to States as outlined in 3.6 above.

**3.8 How will the data be used by these other agencies?**

See 3.6 above.

**3.9 Who is responsible for assuring proper use of the data by other agencies?**

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.

**3.10 How will the system ensure that other agencies only get the information they are entitled to?**

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.

## SECTION 4: QUESTIONS ABOUT MAINTENANCE OF ADMINISTRATIVE CONTROLS

**4.1 Are the data secured consistent with agency requirements under the Federal Information Security Management Act? Specifically:**

**4.1.1 Affirm that the agency is following IT security requirements and procedures required by federal law and policy to ensure that information is appropriately secured.**

The Agency procedures are consistent with the requirements of the Federal Information Security Management Act

(FISMA). FEMA is committed to protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, and destruction in order to provide integrity, confidentiality, and availability of the information. FEMA is completing a Certification and Accreditation on the NEMIS system. In addition, the password protection policies are in accordance with NIST Special Publication 800-63, Electronic Authentication Guideline.

**4.1.2 Acknowledge that the agency has conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls;**

FEMA has conducted a risk assessment and no critical vulnerabilities have been identified. A System Certification and Accreditation is in the final stages of being of completed.

**4.1.3 Describe the monitoring/testing/evaluating on a regular basis to ensure that controls continue to work properly, safeguarding the information.**

The controls protecting this data are an integral part of the NEMIS and are discussed in more detail in Part B of this submission. 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. The baseline system has been operational since 1997.

**4.1.4 Provide a point of contact for any additional questions from users.**

William Prusch
Branch Chief, System Engineering and Development
Federal Emergency Management Agency
500 C Street S.W.
Washington D.C. 20472
(202) 646-2888

**4.1.5 If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

The data from the IA Module is stored in the consolidated master database at FEMA's Mt. Weather facility in Bluemont, VA and in the IA databases at the National Processing Service Centers (NPSCs) located in Denton, Texas, Hyattsville, Maryland, and Mt. Weather. FEMA Headquarters manages data use at all locations. Data consistency is maintained by regular replication of data among the NPSCs and the consolidated master database via automated procedures. FEMA has a configuration management process that is used to deploy the application in a consistent manner throughout the enterprise.

**4.1.6 What are the retention periods of 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. Pursuant to the Government Paperwork Elimination Act (http://www.whitehouse.gov/omb/fedreg/gpea2.html ) and OMB Circular A-130, electronic records are given the same validity as paper-based records. Therefore, the retention periods for data are consistent with retention schedules established by the National Archives and Records Administration (NARA).

**4.1.7 What are the procedures for expunging the data at the end of the retention period and are these procedures documented?**

The data will be destroyed/deleted in accordance with the NARA-approved records retention and disposition schedule established for FEMA records in FEMA Manual 5400.2, Records Management-Files Maintenance and Records Disposition. Electronic records are destroyed/deleted in accordance to the same NARA records retention schedule as the hard copy records.

**4.1.8 Will the system provide the capability to monitor individuals or groups of individuals? If yes, explain.**

Yes, FEMA employs software programs that monitor host and network traffic to identify unauthorized attempts to upload or change information or otherwise cause damage by individuals or group of individuals. 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.

The system has an audit trail of the changes made to the application and the user information associated with that change. Hence, the ability to monitor unauthorized access is provided.

**4.1.9 What controls are in place to prevent unauthorized monitoring of individuals or groups of individuals?**

The FEMA Recovery Division, Individual Assistance Branch strictly controls access to the applicant data using the NEMIS-provided, organizationally structured, role-based access controls for official use only. The controls limiting an individual applicant's access have already been described in detail above.

**4.1.10 Under which Systems of Record Notice (SORN) does the system operate? Provide Number and Name.**

The system currently operates under the already existing Privacy Act system of records, the "Disaster Recovery Assistance Files" (66 FR 195, October 9, 2001).

## SECTION 5: DECISION ANALYSIS

**5.1 Did you evaluate competing technologies on their privacy handling capabilities? If yes, explain.**

No, FEMA has not evaluated competing technologies on their privacy handling capabilities.

**5.2 Were any choice changes made to system architectures, hardware, software, or implementation plans as a result of doing a PIA? If yes, explain.**

No, there were no changes made to system architectures, hardware, software, or implementation plans because of a privacy impact assessment. Security and privacy requirements have always driven the NEMIS architecture, applications, and operations.

# Part B:
# National Emergency Management Information System
# (NEMIS)
# Individual Assistance (IA) Module
# Internet Applications
# Privacy Impact Assessment

**R. Kim/FEMA/OGC/PIA-Pt.A-FINAL-10-6-04-DHS REVIEW-Disaster Assistance-RYK.doc/10-6-04**