



Privacy Impact Assessment for the Disaster Assistance Improvement Program (DAIP)

December 31, 2008

Contact Point

**William S. Prusch
Individual Assistance Branch
Information Technology Division
Federal Emergency Management Agency
(540) 686-3341**

Reviewing Official

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



Abstract

The Department of Homeland Security (DHS) Federal Emergency Management Agency (FEMA) developed the Disaster Assistance Improvement Program (Disaster Assistance Center) in accordance with the August 29, 2006, Executive Order 13411, "Improving Assistance for Disaster Victims." The Disaster Assistance Center is an enhancement and upgrade of the current system known as the National Emergency Management Information System (NEMIS), which contains, stores, and manages information contained in the Disaster Recovery Assistance Files System of Records (DHS/FEMA – REG 2), as announced in the Disaster Recovery Assistance Files System of Record Notice (71 Federal Register 38408, July 6, 2006) (DRA SORN). The data elements include those that are contained and captured on the FEMA form 90-69. The objective of this Privacy Impact Assessment (PIA) is to identify and address the safeguarding of personally identifiable information (PII) that may result from FEMA's proposed implementation of Executive Order 13411, here after known as Disaster Assistance Center DAIP, and its modification of the Individual Assistance Center application.

Overview

Disaster Assistance Center is operated under the executive sponsorship of FEMA's Deputy Administrator and the Deputy Assistant Administrator for the Disaster Assistance Directorate. The purpose of this system is to fulfill the requirements of Executive Order 13411 (E.O. 13411), to simplify the process of identifying and applying for disaster assistance. This mandate and FEMA's mission support DHS's Strategic Goals regarding response and recovery from acts of terrorism, natural disasters, or other emergencies, and recovery efforts to restore services and rebuild communities after acts of terrorism, natural disasters, and other emergencies. The system also enhances the ability of FEMA to prevent duplication of benefits to applicants by sharing applicant information with some of the participating federal agencies in an expeditious manner, enabling them to adjust and/or off-set disbursements to applicants as required under 44 C.F.R. § 206.191.

In order to implement E.O. 13411 and better meet other legal requirements, FEMA is implementing the Disaster Assistance Center. This includes implementation of specific actions to improve the delivery of Federal disaster assistance by providing a centralized application process for Federal disaster assistance for Federal, State, local, tribal, and private disaster assistance information. Disaster Assistance Center will receive a single application for disaster assistance, sort applications based on requirements, and route the application to the appropriate Federal agency. Disaster Assistance Center will use a service from www.GovBenefits.gov to determine the applicant's eligibility for any federal forms of assistance. The GovBenefits service will not use PII. The applicant may use a single universal application for assistance from multiple programs. FEMA owns the program that routes the applications.

Typical Transaction

Individuals requesting disaster assistance utilize the GovBenefits service via <http://www.DisasterAssistance.gov> to determine the specific forms of assistance he/she may be



eligible for or apply directly for FEMA Assistance. When arriving at the site the individual has two options 1) take a ten-question survey to identify the forms of the assistance he/she may be eligible for or 2) start a registration where he/she will complete an online registration, create an account, and apply for assistance. The individual who takes the survey is provided a list of forms of assistance along with the option to apply now, print out, or email descriptions of the forms of assistance. If an individual decides to apply now or start a registration, he/she is transferred to FEMA's Disaster Assistance Center Screen to complete the application process. The actual application process includes a series of prompts for the individual to enter information ranging from his/her name and phone number to home insurance information. For details about the online process, please see Appendix A.

After the applicant submits the application, the Disaster Assistance Center routes the information accordingly. If the Disaster Assistance Center determines that the applicant is requesting assistance from a FEMA program, relevant information will be electronically routed to the NEMIS National Processing Service Center (NPSC) database for processing. For other participating department and agency programs, the Disaster Assistance Center will electronically route relevant applicant information to participating federal agency's systems and be prepared to receive application status information in return.

For FEMA applications, Disaster Assistance Center will take information gathered from the applicant and pass this information to NEMIS for eligibility/ineligibility determinations. Alternately, FEMA's NPSC Call Centers collect the same information and store it electronically in the NEMIS NPSC Database for processing.¹ The NEMIS Individual Assistance (IA) Module currently stores and processes information for the Disaster Recovery Assistance Files System of Records as captured and contained in FEMA Form 90-69 data. The Disaster Assistance Center will assume the role of the IA Module and expand the data collected by the IA module to include the minimum number of elements required to complete a universal, multi-agency application; currently no additional information to that of the FEMA Form 90-69 is collected, except the effective date of the change to the current address.

FEMA's automated business rules determine if an applicant fails the SBA-provided income threshold. In this case, applicants are electronically referred to the Small Business Administration for a low interest loan consideration. This process has been ongoing since the onset of NEMIS and continues under the Disaster Assistance Center processing. The only difference is the Disaster Assistance Center has improved the information exchange design and enforced a higher level security protection. In addition, SBA uses the FEMA provided information to call or otherwise solicit loan applications from the applicants. SBA also returns a status once the applicant's loan eligibility has been determined. Based on this determination, FEMA may provide additional assistance to supplement SBA's assistance.

¹ Disaster Assistance Center Form 90-69a is FEMA's application for Application for Disaster Assistance. The PIA for the electronic collection of Form 90-69 data can be found at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_eprindassist.pdf



90-69 Form

The 90-69 form captures the aggregate data provided by the user during the disaster assistance registration process. It collects such information as full name, home address, current address, social security number, date of birth, bank routing and account information, insurance information, and location of damaged dwelling.

Specifically, the original information is collected from individuals either via telephone interviews with disaster victims who call into a published disaster assistance number, where teleregistrars record their personal application information directly into the NEMIS system.

The information collected on the FEMA 90-69 is covered by the Disaster Recovery Assistance Files System of Record Notice (71 Federal Register 38408, July 6, 2006) (DRA SORN). With updates to this program, FEMA will now be able to share certain information with the Social Security Administration (SSA). The individual will be given a choice during the application process as to whether or not they would like their information shared with SSA, so that he may receive his SSA benefits at the new mailing address provided on the 90-69.

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

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

The information Disaster Assistance Center collects in order to track, evaluate, and provide benefits to the individual applying for disaster assistance includes but is not limited to the following data elements:

- Personal Identification information, such as, name, current mailing address, Social Security Number (SSN), Date of birth.
- Contact Phone Numbers
- Damaged Dwelling Address
- Damaged Dwelling County/Parish/Municipality
- Disaster Selection
- Damage Type
- Disaster Related Loss
- Damaged Dwelling
- Home Insurance
- Disaster Related Expenses
- Disaster Related Vehicle Damage
- Miscellaneous Purchases
- Emergency Needs



- Special Needs
- Occupants
- Business Damages
- Financial Information, such as bank name and account information
- Income
- Pass/Fail indication for identify verification (currently provided by ChoicePoint)

Appendix B is a copy of the FEMA form 90-69.

In addition to the above information collected on the FEMA Form 90-69, FEMA requires individuals to set up security questions so that it can verify an individual, if the individual forgets his password.

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

FEMA secures identity verification (a person with the given credentials exists) and authentication (the person is who he/she says he is) services from ChoicePoint. The services were competitively obtained from among a fairly large number of responses to an open source request for proposals. The appendix contains a briefing that describes the Identity Verification and Authentication process at a high level. FEMA collects full name, address, social security number, and data of birth from disaster applicants and sends an Identity verification query via a secure web service to ChoicePoint. ChoicePoint performs a query of its enormous database of public records to determine if a person with these credentials exists and returns a yes/no status together with any failure modes such as the SSN is of a deceased person, the SSN is invalid, the name and social do not agree, or the SSN is owned by more than one person.

After an applicant has been verified and registers for assistance, the applicant may wish to determine the status of FEMA's processing of their application or they may wish to update, complete or change a few key fields on their application. In order to make these changes and to prevent fraud, FEMA requires the applicant to be authenticated to ensure they are who they say they are. The same four data elements that were presented for Identity Verification is sent once again to ChoicePoint and is used for ChoicePoint to develop a four question quiz. The four question quiz is against out-of-wallet information from the ChoicePoint database of public records. E.g., the quiz might ask the applicant which of the following four streets you have lived on in the past ten years. In order to be authenticated the applicant must answer at least three-of four multiple choice questions correctly.

FEMA considered the use of SSA services for identity verification and authentication, but SSA was unable to meet our requirements. A large conference call between the SSA senior staff and their technical staffs together with OMB, DHSOIG, and FEMA IT Staff came to this conclusion after considerable discussion. Since SSA does not require updates to persons with Social Security



Numbers, they cannot ensure that a person with a given SSN exists or is who they say they are. One good example, is that SSA does not know when a female gets married and changes their name.

If an applicant fails the ChoicePoint checks for identity, they can still complete a registration through our call center. When an Individual and Households Program (IHP) eligibility decision is made for that applicant, if they have not passed identity verification, they will receive an ineligible decision paragraph telling them that we were unable to verify their identity, as well as what documentation they can provide in order to overturn the identity verification failure. We don't provide the information from ChoicePoint back to the applicant, as we don't have the detail of why they failed the check. All we receive is a Pass or Fail flag with reason codes for issues with the SSN.

If the applicant fails the ChoicePoint authentication quiz, the applicant is instructed to call the call center, where the teleregistrar retrieves the applicant's application and asks a series of questions from the details of the application to ensure the applicant submitted the application. If the applicant answers the questions, they will be given a general status of their application and be allowed to change their current mailing address. Otherwise, they are asked to mail-in proof of a change to their SSN or Bank Account information, before this information will be changed. Again, we don't provide the information from ChoicePoint back to the applicant, as we don't have the detail of why they failed the check.

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

The collection of such PII is necessary for FEMA and cooperating entities to carry out their mission of assisting individuals who apply for disaster assistance benefits under the Robert T. Stafford Disaster Relief and Emergency Assistance Act. Specifically, the collection of Social Security Numbers is necessary to identify applicants who forget their registration identifier and to perform identity verification and authentication. Identity verification and authentication services are highly inaccurate without the use of Social Security Numbers.

1.4 How is the information collected?

The Disaster Assistance Center collects information based on FEMA Form 90-69 and stores it electronically in the NEMIS NPSC Database. To access FEMA programs, applicants requesting disaster assistance have the option to provide information directly to the Disaster Assistance Center in one of three ways described below:

- 1) Telephone interview - Applicants call FEMA through a published disaster assistance phone number and a FEMA teleregistrar reads questions and enters data directly into NEMIS on behalf of the applicant;
- 2) Internet - Applicants provide the same information that would be collected by the telephone interview processes to a FEMA web site via a 128-bit encrypted secure



connection Disaster Assistance Center will send information required for eligibility determination and subsequently for payment requests to the NEMIS system. In all cases, the same type of PII goes into Disaster Assistance Center for eligibility processing or is sent over 128 bit-encrypted communications to partner agency processing systems.

3) Hardcopy – On rare occasions, applicants will be given a hardcopy of the 90-69 form for submission to Disaster Assistance Center. The information is certified by signing FEMA Form 90-69B “Declaration and Release.” The information, once received by the NPSC designated by the Disaster Assistance Directorate, will be entered into the Disaster Assistance Center by a teleregistrar, scanned and associated with the electronic application and destroyed.

1.5 How will the information be checked for accuracy?

When a user initiates a request for disaster assistance, NEMIS collects the applicant’s full name, damaged dwelling address, social security number, and date of birth to be used to verify their identity. This information is sent to ChoicePoint (CP), a commercial data service provider’s system, in a secure manner for identity verification. A status of Pass/Fail is returned from CP. The CP Identity Verification solution employs a variety of data sources, including live gateway access to critical identity verification data. The solution is designed to achieve the highest level of assurance regarding the accuracy of identifying information on individuals applying for assistance. CP is also capable of providing results in a timely manner of six seconds or less to assist FEMA in granting or denying assistance.

Since individuals personally complete the on-line and hardcopy applications, the information is assumed to be accurate. Likewise, individuals who opt to use the telephone application process provide information to the teleregistrar who in turn will enter the data into the system. CP provides screen pre-population data to the teleregistrars that helps ensure the data accuracy. Thus, the level of accuracy is estimated to be high. CP can automatically populate the registration forms with data matched from CP public record and proprietary sources. Using data pre-population reduces the need for manual entry of data, such as addresses, telephone numbers, and property information, thus also reducing the number of data entry errors.

Applicants are sent a hard copy printout of their application and, therefore, always have the opportunity to correct errors and update information. Since the applications are the source of the information being entered into the system, it is assumed they will verify the accuracy of information entered. Integrity is maintained by implemented security controls for auditing in accordance with DHS policy.

Once information collected it is processed through initial eligibility rules, field disaster housing inspections, verification and post-inspection eligibility rules or manual case processing, the individual's record is automatically updated to reflect the status of their specific application by FEMA and/or each Disaster Assistance Center partner agency. Examples of the status of an application would be “in process,” “submitted” or “approved.”



The disaster victim who supplies the data originally only has access to his/her own personally identifiable information (PII). The disaster victim validates their own information at the time of initial submission of their own application. Each applicant establishes a user id and password, and FEMA's NEMIS provides a personal identification number (PIN), in order to gain subsequent limited access only to their own data. Only applicants that wish to gain subsequent access will need to create an account and receive a PIN. Otherwise, no account or PIN is required.

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

Legal requirements to address privacy issues are derived from the following references:

SSNs are collected as an electronic analog of Form 90-69 and are used to prevent the duplication of disaster benefits among FEMA, Federal, and state and local disaster agencies. 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 C.F.R.) 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 order to provide assistance to victims of a disaster, the DHS/FEMA Disaster Assistance Center 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 electronic National Emergency Management Information System (NEMIS) Individual Assistance Module, which hosts Disaster Assistance Center, 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) § 1702
- Computer Fraud and Abuse Act of 1986, public law 99-474, 18 U.S.C. § 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
- NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories
- FIPS PUB 140-2, Security Requirements for Cryptographic Modules
- FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems

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

Application inflow to Disaster Assistance Center is projected to handle over 1,000,000 applications annually. 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. In view of the amount and type of data being collected, unauthorized system access poses the greatest privacy risk to the confidentiality and integrity of the data collected and stored by the Disaster Assistance Center. This risk has been mitigated by the implementation encryption and auditing protections of applicant information. Data submission via the Disaster Assistance Center is protected using the Secure Socket Layer protocol and encryption. Additional discussions of system security protections for the Disaster Assistance Center are discussed in Section 8.0 of this PIA.

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");
- Computer Security Act of 1987, Public Law 100-235, 40 U.S.C. § 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).

FEMA has set up a system with a commercial data provider, so that the commercial data provider is collecting information it needs to provide identity verification, but FEMA does not need to collect this information. FEMA has also put in place contractual agreement with ChoicePoint that ChoicePoint may not maintain the information related to the FEMA query for its own purposes or to be incorporated or used by any other entity.

Section 2.0 Uses of the Information

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

2.1 Describe all the uses of information.

The applicant information will be used to determine eligibility for assistance and if eligible to provide assistance to individuals who are victims of a disaster. The information collected will be used for inspection management, which verifies applicant damage claims and assesses the repair or replacement costs. Applicants will be required to submit supporting documents such as driver's license with picture ID, property title, tax bill or utility bill for proof of occupancy. Information will be used to provide summarized temporary housing when required. Summarized information will be used for program administration purposes including: budgeting, sheltering, prioritizing assistance, and reporting to oversight organization.

ChoicePoint, the current contractor providing identity verification services, may not use the information for any purpose beyond the FEMA verification services and for accounting purposes for the life of the contract.

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

Disaster Assistance Center does not use any tools or methods, automated or manual, to analyze data or perform tasks that result in data matching, scoring, reporting or pattern analysis. Further, the system does not create or make available new or previously unutilized information about an individual.



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

When a user initiates a request for disaster assistance the applicant is asked for name, address, SSN and date of birth. This data is sent to ChoicePoint to verify that a person with these attributes exists and the SSN is valid.

Should an applicant wish to create an account for the purpose of coming back to check on a detailed status of their applicant processing or to perform limited updates to the information they provided earlier, the information mentioned above is used by ChoicePoint to generate four out-of-wallet questions, to authenticate the applicant. The response to the security questions is sent to CP with the SSN for identification verification. Once the applicant takes the quiz, a status of pass or fail is returned from CP. FEMA does not know the questions or the answers and merely receives a “pass/fail” indication from ChoicePoint. The solution is designed to achieve the highest level of assurance that the identity is reliable and has the ability to return the results in the fastest obtainable timeframe in order for FEMA to grant or deny assistance.

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’s use of a commercial data provider to provide identity verification poses a risk that an individual will be denied the benefit of creating an account because of inaccurate information. In order to mitigate this risk, individuals are given an opportunity to follow up with FEMA directly.

There is also a risk that ChoicePoint could use the information for purposes other than those specifically stated by FEMA; however, FEMA has put in place contractual arrangement stating that FEMA may not use the information for any purpose other than providing FEMA a response and for accounting for the use of the service.

All individuals who maintain and access Disaster Assistance Center are mandated to take Security Awareness Training annually and acknowledge the rules of behavior for using FEMA information technology systems. Additionally, supervisor approved role-based access technical controls are used to strictly control access to the system. Operational and management controls are in place in accordance with DHS policy and users are required to sign a Rules of Behavior agreement before system access is granted. Data confidentiality and integrity are preserved by using encryption, digital signatures and auditing.



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?

Disaster assistance request information will be retained in accordance with the National Archives Records Administration's (NARA) records retention schedule and FEMA's Records Schedule N1-311-86-1, item 4C10a. All information captured by the applicant on FEMA Form 90-69 will be retained for this period.

The identity verification contractor, ChoicePoint may only maintain the information for cost accounting purposes for the length of the contract.

3.2 How long is information retained?

All PII stored in the database is retained for six years and three months after the last log-in to the website occurs, which is consistent with NARA's Government Records Schedule and FEMA Records Schedule N1-311-86-1, item 4C10a.

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

The retention schedule is approved and consistent with NARA's Government Records Schedule and FEMA Records Schedule N1-311-86-1, item 4C10a. Records will be destroyed after six years and three months.

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

The risks associated with the length of time data is retained include misuse of data, loss of data, inadvertent release of data, and identify theft. Risks are minimized by limiting who has access to data, minimizing when and how access is provided, securing the information both in transit (mobile) and at rest in accordance with encryption standards listed in FIPS 140-2. Database auditing is used to monitor database access. Policies covering operational and technical safeguards are in place to preserve the integrity and confidentiality of archived data.



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

The organization internal to FEMA that uses the data collected in Disaster Assistance Center is the Disaster Assistance Directorate, Individual Assistance Division. The information is used to provide assistance to individuals affected by a disaster. The information is consolidated into reports but does not include PII. For example, a report indicating the number of registrations on a given day may be used by upper management. The FEMA regional and Joint Field Offices (JFO) IA staff have IA functions that utilize the reports as well.

4.2 How is the information transmitted or disclosed?

Information is shared internally for purposes of auditing and to provide management reports. Sharing of data internally is strictly controlled and policies implemented to insure the proper handling of data. This information is transmitted via email, phone or hard copy by and to authorized personnel.

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.

FISMA requires all individuals with access to Disaster Assistance Center to annually participate in DHS/FEMA's mandated Information Assurance (IA) role based training. Access controls are used to strictly control access to the system. Appropriate operational and management controls are in place in accordance with DHS policy. Users of the system are required to sign a Rules of Behavior agreement before system access is granted. Data confidentiality is preserved by applying federally approved cryptographic requirements appropriate for the security categorization of the system. Auditing technical controls are in place and are regularly reviewed. Formal risk analyses are periodically conducted as part of the certification of the system. Appropriate security controls such as auditing and encryption will be implemented to mitigate risks and ensure that data is protected within the FEMA system. An annual risk assessment will be conducted to assess and implement additional security controls as the threat landscape changes.



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 that 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 purpose?

FEMA works closely with and shares selected data with the Small Business Administration (SBA). Formalized agreements are in place with SBA for the information sharing to be limited to "official use" only for FEMA and SBA purposes. Initially, the following agencies will be using Disaster Assistance Center: Social Security Administration (SSA), Small Business Administration (SBA), Department of Education (ED), and Department of Labor (DOL). In subsequent phases, the following agencies may be using Disaster Assistance Center: Department of Housing and Urban Development (HUD), Department of Agriculture (USDA), Department of Health & Human Services (HHS), Department of Justice (USDOJ), Department of the Interior (DOI), Department of Treasury (Treasury), Department of Veterans' Affairs (VA), and Office of Personnel Management (OPM). Below is a description of what data is shared:

- SSA: FEMA passes disaster related change of address and it's effective date
Prior to sending the information to SSA the user will be prompted with the acknowledgment of SSA sharing prior to final submittal of the application. The Disaster Assistance Improvement Program (DAIP) will exchange change of address (current address from FEMA 90-69 application) and the effective date of the current address change (a new field that has been added to the 90-69) data with the Social Security Administration (SSA). The change of address information will be collected so disaster victims, who are also Social Security beneficiaries, can have their benefits checks sent to their temporary or new residence following a major or catastrophic disaster situation. Only disaster victims who have registered for FEMA individual assistance and are existing Social Security beneficiaries will be allowed to update their change of address via DisasterAssistance.Gov or its supporting call centers.
- SBA: FEMA will pass disaster applicant information, for applicants who exceed the SBA provided income threshold, to the Small Business Administration Disaster Credit Management System for low-interest loan consideration. Once a loan determination is made, SBA will pass status information back to FEMA. FEMA may provide additional assistance based on SBA's determination.
- DoED: Will include web redirect to enable user to access student loan status
This applicant is redirected so he can access an existing Dept. of Education National Student Loan Data System account created separate from Disaster Assistance Center. This transaction posts the Disaster Assistance Center user's data to the target landing URL provided by DoED. DoED will prepopulate the first two characters of the last name, SSN, and DOB using this information and allow the user to enter their PIN to proceed with accessing their student loan data. DoED will also provide a link or a button to log out of the NSLDS session, close the



window, and return to Disaster Assistance Center. With this process an applicant impacted by a catastrophic disaster, who has lost their student loan records, will have access to their student loan information thru a common application.

- DOL: will pass information pertaining to benefit programs available to the applicant based on questions answered by the user (no PII is passed)

Once an applicant is approved for FEMA assistance the applicant is also referred to SBA for assistance. The data is securely transmitted from FEMA to SBA so the applicant can apply for a small business and/or personal loan to assist in mitigating the results of a federal declared disaster. Personal information such as name, address, social security number, assets and salary are securely transmitted from FEMA to SBA for processing. SBA will return back a status code for each application received from FEMA. Examples of a status code would be rejected, approved, declined, verified or cancelled.

Agencies participating in the Disaster Assistance Improvement Program are granted limited access to information as it relates to their program. In all cases, access to the data is limited and controlled on a need-to-know basis. Only authorized FEMA officials have access to the composite data source.

In addition to the above sharing with government agencies, FEMA has contracted with an identity verification company, ChoicePoint. Individuals provide information to ChoicePoint and the information that FEMA receives back is information related to whether or not the individual passed or failed the authentication quiz.

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.

Routine Uses and the sharing of PII collected and maintained in the Disaster Assistance Center are documented in the DHS/FEMA – REG 2, DRA SORN. Additionally, a Memorandum of Understanding (MOU) and Interconnects Security Agreement (ISA) between FEMA and each participating agency defines the conditions for security and use of data from data exchanges to the extent they are not covered by other formal arrangements or agreements between the Parties. This agreement also covers any existing data exchanges covered in the DHS/FEMA – REG 2 DRA SORN. The DAIP has agreed to update the SORN to reflect the Disaster Assistance Center exchange of information with SSA. For the interim, prior to sending the information to SSA, the user will be prompted to consent with FEMA sharing their change of address data with SSA. In addition, while the current SORN has a routine use to provide information to contractors, it is considered a best practice to provide more explicit routine uses in the SORN, as such FEMA will be including a



routine use related to the collection of information by a commercial provider, ChoicePoint, for identity verification.

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

The MOU between FEMA and each participating agency covers security requirements for transmission of data. Additionally, Service Level Agreements (SLA), and Interconnections Security Agreement (ISAs) are in place detailing technical requirements on transmission and security of data between FEMA and each partner agencies.

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

The Disaster Assistance Center provides a secure environment for application communications between FEMA and each agency. The Disaster Assistance Center utilizes a standards-based security protocol of a Service Oriented Architecture (SOA) to mitigate the privacy risk through the SOA's interoperability with a large number of system interfaces and data formats. The MOUs, SLAs and ISAs between FEMA and each participating agency will cover security requirements for transmission of data containing PII. The security requirements include encryption of PII during transmission between FEMA and external agencies and protection of data within the participating agencies' system. Details on how data is secured will be documented in the ISAs. Individuals requesting information have access to only the information they have submitted themselves. FEMA will review these interconnection agreements on an annual basis and review appropriate security documents for any newly identified risks. Any newly identified risks will be mitigated between the partnering agencies in accordance with applicable laws.

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?

Notice is provided by way of DHS/FEMA – Reg 2 DRA SORN. A Privacy Act Statement will be provided in hardcopy or electronic form to individuals requesting assistance that includes the disclosure of routine uses for FEMA. The notice consist of FEMA's general Privacy Act Statement and further notice regarding sensitive PII. The DAIP has agreed to update the SORN to reflect the Disaster Assistance Center exchange of information with SSA as well as the use of a commercial data provider to provide identity verification. For the interim, prior to sending the information to SSA, the user will be prompted to consent with FEMA sharing their change of address data with SSA.



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

Yes. However, the individual is also advised that failure to submit the necessary PII may result in the denial of disaster assistance.

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

Consent to use the information is implied by the individual requesting assistance.

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.

Individuals requesting disaster assistance are notified of the potential use of their PII prior to the submission of application information and through publication of the DHS/FEMA- DRA SORN. Notification is provided in two forms: 1) verbal notification at the beginning of the phone interview, or 2) warning banner notification for online applications. The risk of individuals being unaware of the collection of their information is minimal to none since the individual or their representative is providing the information. Therefore, they are fully aware of the information collection and use of their PII as specified in the privacy act statement and the DHS/FEMA- Reg 2 "Disaster Recovery Assistance Files" SORN. The risk is mitigated by the user acknowledging that he/she has read the privacy statement and agrees to the terms and conditions.

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?

Applicants can access their information in one of three ways: (1) applicants may access their information on-line using the user id, password, a system generated PIN and authentication that was established during the application process; (2) Applicants may call to check on the status of their application by providing the registration ID (3) if on-line access is not available, applicants may submit a Privacy Act request pursuant to DHS' Privacy Act Regulations, 44 C.F.R. § 6 and 6 C.F.R. § 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 sent to the Disclosure Officer, DHS/FEMA, Records Management Division, 500 C Street, SW, Washington, DC 20472.

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

Correction of inaccurate data may be made by the individual on-line by authenticating into the system and making the appropriate corrections. If on-line access is not available, individuals should notify FEMA of the error/inaccuracy and provide FEMA with the correct information. Send requests to the Disclosure Office at the location listed above. For data that needs to be corrected from an external agency, a request can be made to that agency in accordance with their applicable policies. Some examples of data correction may be due to duplicate entries, system errors or a security breach.

If an applicant fails the ChoicePoint checks for identity, they can still complete a registration through our call center. When an Individual and Households Program (IHP) eligibility decision is made for that applicant, if they have not passed identity verification, they will receive an ineligible decision paragraph telling them that we were unable to verify their identity, as well as what documentation they can provide in order to overturn the identity verification failure. We don't provide the information from ChoicePoint back to the applicant, as we don't have the detail of why they failed the check. All we receive is a Pass or Fail flag with reason codes for issues with the SSN.

If the applicant fails the ChoicePoint authentication quiz, the applicant is instructed to call the call center, where the teleregistrar retrieves the applicant's application and asks a series of questions from the details of the application to ensure the applicant submitted the application. If the applicant answers the questions, they will be given a general status of their application and be allowed to change their current mailing address. Otherwise, they are asked to mail-in proof of a change to their SSN or Bank Account information, before this information will be changed. Again, we don't provide the information from ChoicePoint back to the applicant, as we don't have the detail of why they failed the check.

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

Individuals are notified of the procedures for correcting information prior to the collection of information, the DHS/FEMA- "DRA" SORN, and this PIA.

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

Redress is provided to individuals requesting assistance.



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

Access and other procedural rights are provided for in the Privacy Act of 1974. The risks associated with the redress include misuse of data, loss of data, inadvertent release of data, and identify theft. Risks can be minimized by limiting accessibility to data, minimizing when and how access is provided, and securing the information both in transit (mobile) and at rest in accordance with the encryption standards listed in FIPS 140-2.

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?

FEMA employees and authorized Information Technology (IT) contractors will have restricted access to Disaster Assistance Center only to the extent necessary to perform their official duties. IT contractors handling the operations and maintenance of the system will also have limited access to the system to support the troubleshooting of technical system issues encountered on a day-to-day basis. FEMA's Integrated Security and Access Control System implements the security access controls and administers users' roles and permissions based on organizational position, which are assigned and approved by the employee's supervisors.

Roles:

- System, Network and Database Administrators – Responsible for maintenance of the system. Roles are defined in System Security Plan
- Information Systems Security Officer – Responsible for overall security posture of Disaster Assistance Center and Certification of the system
- FEMA Security Operations Center (SOC) – Responsible for monitoring and reporting security incidents
- End Users/Applicants – General users with limited access. End users can only access their PII and see content determined by their role in the system

Additionally, all internal end users are required to read and sign a rules of behavior agreement



8.2 Will Department contractors have access to the system?

FEMA information technology staff and developers who manage the operations and maintenance of the Disaster Assistance Center system have controlled role-based access to the data. This is in addition to their FEMA usernames and passwords, in order to view and/or trouble-shoot any technical system or data issue that is brought to their attention.

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

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. Supplementary security-related training is provided for those with additional security-related responsibilities.

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

The system is undergoing a re-certification with the enhanced features. The existing NEMIS Individual Assistance Module is enhanced to include the open web architecture using a Service Oriented Architecture solution.

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

Because unauthorized attempts to upload or change information are prohibited and are 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 to users in the system. The system maintains an audit trail of all changes made to any application including the user information associated with alterations. If an unauthorized user is detected, FEMA may revoke access to that user registration. As previously described in Section 8.1, access to data in the system is restricted. Individuals are approved access only to their own disaster assistance request information. Incident response procedures are established to address reported security incidents as quickly as possible. Additionally, FEMA has established procedures for the handling and storage of information which restricts access to unauthorized users.

In addition to the foregoing privacy-related documents, FEMA's electronic National Emergency Management Information System (NEMIS) Individual Assistance Module, which hosts Disaster Assistance Center, 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) § 1702
- Computer Fraud and Abuse Act of 1986, Public Law 99-474, 18 U.S.C. § 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
- NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories
- FIPS PUB 140-2, Security Requirements for Cryptographic Modules
- FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems

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?

FEMA will apply appropriate operational, management, and technical security controls to the Disaster Assistance Center system to insure proper user authentication, confidentiality and integrity of data preservation, and appropriate placement of auditing and incident response. All security controls will be implemented in accordance with DHS/FEMA security policy.



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 What type of project is the program or system?

The project is a web-enabled system using a secure open framework.

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

Per DHS System Life Cycle (DHS SLC v.9), the system is currently in the requirements definition phase. The system is scheduled to be operational by 31 December 2008.

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 PII. A risk assessment will be conducted periodically to identify current and emerging threats and mitigate any risks associated with the architecture.

Approval Signature

Original signed and on file with the DHS Privacy Office

Hugo Teufel III

Chief Privacy Officer

Department of Homeland Security



APPENDIX A: The Disaster Assistance Center Process

- User accesses <http://www.DisasterAssistance.gov>
- From the landing page (hosted by GovBenefits), the user can switch to a Spanish version of the site, can perform a search, can click on top-level menu items to get more information on Disaster Assistance, About Us, Help, or can click on buttons to “Take Questionnaire,” “Start Registration,” or “Login” (to check application status)
 - Searching will search government sites for keyword entered
 - Top level menu items provide additional information about the site, including additional resources, partner information, search of forms of assistance by category and by federal agency, Frequently Asked Questions (FAQs), and Contact Us details
 - “Take Questionnaire” allows user to take a 10 question survey that helps identify the forms of assistance for which the user may be eligible
 - “Start Registration” allows the user to immediately begin registering for FEMA housing assistance
 - Login allows the user to access the FEMA Disaster Assistance Center (DAC) to check the status of a registration either previously entered via DisasterAssistance.gov or given through the FEMA Disaster Assistance call center
- By clicking on “Take Questionnaire” the user answers 10 questions, clicks a “Submit” button, and is returned with the list of forms of assistance for which they may be eligible
 - “Forms of Assistance You can Apply for Online” shows everything the user may apply for electronically
 - “Forms of Assistance Without Online Applications” shows everything the user may qualify for that does not have electronic application. Expanding detail on these forms of assistance will give the user more information on the assistance provided and how to apply
 - The user is given the option to print or email these lists to from this page
 - The user can click an “Apply Now” button to begin the registration process for online forms of assistance
- By clicking on the “Apply Now” button, the user is presented with a confirmation screen, asking them to verify that they do indeed want to begin the application process, and informing the user that they will not be able to return to their results screen
 - The user can click “Apply Now” button
 - The user can click “Back to Results” button, which returns user to the list of forms of assistance for which they may be eligible
- By clicking the “Apply Now” button on the verification screen (or the “Start Registration” button from the Landing Page), the user is transferred to the Disaster Assistance Center Screen (hosted by FEMA). This screen explains the application process and what information is needed to apply
 - The user can view this screen in English or Spanish
 - The user can click a button to “Cancel” the registration process
 - The user can click a button to “Start” the application process
- By clicking the “Start” button, the user is presented with a screen that gives instructions for the application process.
 - The user can click a button to “Delete this Registration”



- Clicking on this button produces a validation screen to verify user wants to cancel process
 - User can click “No” and return to application process
 - User can click “Yes” and exit application process with no record of application remaining in system
 - User is provided call center number to apply via telephone
- The user can click a “Next” button to continue
- By clicking on “Next” button, user is presented with Privacy Act screen. User is required to check a box to indicate acceptance of the Privacy Act
 - The user can click a “Back” to return to previous page
 - The user can click a button to “Delete this Registration”
 - Clicking on this button produces a validation screen to verify user wants to cancel process.
 - User can click “No” and return to application process
 - User can click “Yes” and exit application process with no record of application remaining in system
 - User is provided call center number to apply via telephone
 - The user can click a “Next” button to continue
- By clicking on “Next” button, user is presented with **Personal Identification** screen. User must input requested data
 - The user can click a “Back” to return to previous page
 - The user can click a button to “Delete this Registration”
 - Clicking on this button produces a validation screen to verify user wants to cancel process.
 - User can click “No” and return to application process
 - User can click “Yes” and exit application process with no record of application remaining in system
 - User is provided call center number to apply via telephone
 - The user can click a “Next” button to continue
- By clicking on “Next” button, user is presented with **Contact Phone Numbers** screen. User must input requested data
 - The user can click a “Back” to return to previous page
 - The user can click a button to “Delete this Registration”
 - Clicking on this button produces a validation screen to verify user wants to cancel process.
 - User can click “No” and return to application process
 - User can click “Yes” and exit application process with no record of application remaining in system
 - User is provided call center number to apply via telephone
 - The user can click a “Next” button to continue
- By clicking on “Next” button, user is presented with **Damaged Dwelling Address** screen. User must input requested data
 - The user can click a “Back” to return to previous page
 - The user can click a button to “Delete this Registration”
 - Clicking on this button produces a validation screen to verify user wants to cancel process.
 - User can click “No” and return to application process



- User can click “Yes” and exit application process with no record of application remaining in system
 - User is provided call center number to apply via telephone
 - The user can click a “Next” button to continue
 - By clicking on “Next” button, user is presented with **Damaged Dwelling County/Parish/Municipality** screen. User must enter/validate requested data
 - The user can click a “Back” to return to previous page
 - The user can click a button to “Delete this Registration”
 - Clicking on this button produces a validation screen to verify user wants to cancel process.
 - User can click “No” and return to application process
 - User can click “Yes” and exit application process with no record of application remaining in system
 - User is provided call center number to apply via telephone
 - The user can click a “Next” button to continue
 - By clicking on “Next” button, user is presented with **Disaster Selection** screen. User must input requested data
 - The user can click a “Back” to return to previous page
 - The user can click a button to “Delete this Registration”
 - Clicking on this button produces a validation screen to verify user wants to cancel process.
 - User can click “No” and return to application process
 - User can click “Yes” and exit application process with no record of application remaining in system
 - User is provided call center number to apply via telephone
 - The user can click a “Next” button to continue
 - By clicking on “Next” user is presented with **Damage Type** screen. User must input requested data
 - The user can click a “Back” to return to previous page
 - The user can click a button to “Delete this Registration”
 - Clicking on this button produces a validation screen to verify user wants to cancel process.
 - User can click “No” and return to application process
 - User can click “Yes” and exit application process with no record of application remaining in system
 - User is provided call center number to apply via telephone
 - The user can click a “Next” button to continue
 - By clicking “Next” user is presented with **Disaster Related Loss** screen. User must input requested data
 - The user can click a “Back” to return to previous page
 - The user can click a button to “Delete this Registration”
 - Clicking on this button produces a validation screen to verify user wants to cancel process.
 - User can click “No” and return to application process
 - User can click “Yes” and exit application process with no record of application remaining in system
 - User is provided call center number to apply via telephone



- The user can click a “Next” button to continue
- By clicking “Next” button user is presented with **Damaged Dwelling** screen. User must input requested data
 - The user can click a “Back” to return to previous page
 - The user can click a button to “Delete this Registration”
 - Clicking on this button produces a validation screen to verify user wants to cancel process.
 - User can click “No” and return to application process
 - User can click “Yes” and exit application process with no record of application remaining in system
 - User is provided call center number to apply via telephone
 - The user can click a “Next” button to continue
- By clicking “Next” button user is presented with **Home Insurance** screen. User must input requested data
 - The user can click a “Back” to return to previous page
 - The user can click a button to “Delete this Registration”
 - Clicking on this button produces a validation screen to verify user wants to cancel process.
 - User can click “No” and return to application process
 - User can click “Yes” and exit application process with no record of application remaining in system
 - User is provided call center number to apply via telephone
 - The user can click a “Next” button to continue
- By clicking “Next” button user is presented with **Disaster Related Expenses** screen. User must input requested data
 - The user can click a “Back” to return to previous page
 - The user can click a button to “Delete this Registration”
 - Clicking on this button produces a validation screen to verify user wants to cancel process.
 - User can click “No” and return to application process
 - User can click “Yes” and exit application process with no record of application remaining in system
 - User is provided call center number to apply via telephone
 - The user can click a “Next” button to continue
- By clicking “Next” button user is presented with **Disaster Related Vehicle Damage** screen. User must input requested data
 - The user can click a “Back” to return to previous page
 - The user can click a button to “Delete this Registration”
 - Clicking on this button produces a validation screen to verify user wants to cancel process.
 - User can click “No” and return to application process
 - User can click “Yes” and exit application process with no record of application remaining in system
 - User is provided call center number to apply via telephone
 - The user can click a “Next” button to continue
- By clicking “Next” button user is presented with **Miscellaneous Purchases** screen. User must input requested data



- The user can click a “Back” to return to previous page
- The user can click a button to “Delete this Registration”
 - Clicking on this button produces a validation screen to verify user wants to cancel process.
 - User can click “No” and return to application process
 - User can click “Yes” and exit application process with no record of application remaining in system
 - User is provided call center number to apply via telephone
- The user can click a “Next” button to continue
- By clicking “Next” screen user is presented with **Emergency Needs** screen. User must input requested data
 - The user can click a “Back” to return to previous page
 - The user can click a button to “Delete this Registration”
 - Clicking on this button produces a validation screen to verify user wants to cancel process.
 - User can click “No” and return to application process
 - User can click “Yes” and exit application process with no record of application remaining in system
 - User is provided call center number to apply via telephone
 - The user can click a “Next” button to continue
- By clicking “Next” button user is presented with **Special Needs** screen. User must input requested data
 - The user can click a “Back” to return to previous page
 - The user can click a button to “Delete this Registration”
 - Clicking on this button produces a validation screen to verify user wants to cancel process.
 - User can click “No” and return to application process
 - User can click “Yes” and exit application process with no record of application remaining in system
 - User is provided call center number to apply via telephone
 - The user can click a “Next” button to continue
- By clicking “Next” button user is presented with **Occupants** screen. User must input requested data
 - User can click “Add” button to input information about additional residents of dwelling. Button can be clicked as many times as necessary to input data about all members of household
 - The user can click a “Back” to return to previous page
 - The user can click a button to “Delete this Registration”
 - Clicking on this button produces a validation screen to verify user wants to cancel process.
 - User can click “No” and return to application process
 - User can click “Yes” and exit application process with no record of application remaining in system
 - User is provided call center number to apply via telephone
 - The user can click a “Next” button to continue
- By clicking “Next” button user is presented with **Business Damages** screen. User must input requested data



- The user can click a “Back” to return to previous page
 - The user can click a button to “Delete this Registration”
 - Clicking on this button produces a validation screen to verify user wants to cancel process.
 - User can click “No” and return to application process
 - User can click “Yes” and exit application process with no record of application remaining in system
 - User is provided call center number to apply via telephone
 - The user can click a “Next” button to continue
 - By clicking “Next” button user is presented with **Financial Information** screen. User must input requested data
 - The user can click a “Back” to return to previous page
 - The user can click a button to “Delete this Registration”
 - Clicking on this button produces a validation screen to verify user wants to cancel process.
 - User can click “No” and return to application process
 - User can click “Yes” and exit application process with no record of application remaining in system
 - User is provided call center number to apply via telephone
 - The user can click a “Next” button to continue
 - By clicking “Next” button user is presented with Income Verification screen. User must input requested data
 - The user can click a “Back” to return to previous page
 - The user can click a button to “Delete this Registration”
 - Clicking on this button produces a validation screen to verify user wants to cancel process.
 - User can click “No” and return to application process
 - User can click “Yes” and exit application process with no record of application remaining in system
 - User is provided call center number to apply via telephone
 - The user can click a “Next” button to continue
 - By clicking “Next” button user is presented with Program Referrals screen. User is informed that their application is complete, and is presented with additional program referrals based on their application answers
 - User can click on “Next” button
 - By clicking on “Next” button user is presented with Assistance from Other Agencies or Organizations screen. This shows user the same information presented from the questionnaire earlier in the process for the forms of assistance without online applications, as well as additional referrals identified by FEMA
 - The user can click a “Back” to return to previous page
 - The user can click a “Next” button to continue
 - By clicking on “Next” button user is presented with Conclusion screen. User is given registration number and disaster ID number
 - User can print summary of registration information
- User can click on button to “Create” account to check status of application(s).



Additional Information on NEMIS

The Federal Emergency Management System (FEMA) Individual Assistance (IA) Program provides disaster recovery assistance to individuals and businesses after a Federally declared disaster or FEMA-declared Emergency Declaration based on the requirements of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act). The automation of these services is implemented in a series of services and modules within the National Emergency Management Information System (NEMIS). NEMIS is FEMA's legacy integrated disaster management support capability which has provided both mission application support and system platform services support for every declared disaster or emergency since 1998. The Mission Application Platform Services are being separated from the supporting applications so that each application and the platform can independently evolve to meet the evolving mission requirements and technology changes. Although the integrated NEMIS continues to meet FEMA's legacy needs, modernization requirements, new requirements, and expansion of existing requirements necessitates the new development, integration, and sustainment services. These services for the Individual Assistance Program are vested in the Individual Assistance Program Support Systems (IAPSS). IAPSS is composed of the following modules:

- a. Admin Tool – Used to setup the initial disaster configuration for the entire IAPSS.
- b. Assistance Client – Provides the ability for manual application processing when required.
- c. Automated Construction Estimate (ACE 3) – Field tablet PC software and supporting data communication supporting FEMA housing inspection services contractors to perform field housing inspections and registration intake.
- d. Auto-Determination – The automated business rules used to determine individual and household eligibility based on the Robert T. Stafford Act. There are over 1,000 business rules in NEMIS that determine how registrations (applications for assistance) flow through the system and are processed.
- e. Call Center Registration Intake (RI) and Helpline – Software supports teleregistrars who interface with citizens who call one of FEMA's four permanent or multiple governmental or commercial surge call centers to apply for assistance or to inquire about the status of their application.
- f. Internet Assistance Center (IAC) – Internet portal software provides the capability for citizens to apply for assistance or to receive the status of their application through the Internet. This application must support 30,000 concurrent users and include provision to on-demand services to surge support for up to 200,000 concurrent users.
- g. Mail Utility – Software supports the generation and management of letter printing to support disaster processing.
- h. Mailroom – Software supports manual and automated scanning and indexing for incoming applicant information via mail and fax as well as placement of the information in the applicant's case file and automatically routing the case file to the appropriate processing queue.

This system is operational. The current system requires the continuous minor adjustments and changes that accompany any large multi-user product of this type that is continuously evolving. This effort includes integration of activities with the software processes/modules. Included as part of IAPSS are several applications that have been developed to support reporting and local National Processing Service Center requirements.



Application/Registration for Disaster Assistance Instructions

1. Enter the last name, first name, and middle initial of the applicant. Jr., Sr., etc. follow the last name.
2. Enter the language that the applicant speaks. If the applicant speaks English, leave blank.
3. Enter the date of birth of the applicant.
4. Enter the applicant's social security number (SSN). If the applicant does not provide a SSN, processing of the applicant may be delayed.
5. Enter e-mail address (if available).
6. Do NOT include a beeper/pager number in any of the phone number fields. Damaged Phone number: enter the phone number used in the applicant's home at the time of the disaster even if the number is currently working.
7. Current Phone No. Enter the current phone number where the applicant can be reached. Alternate/Cell Phone No.: enter a work phone number or the phone number of a friend, relative, or neighbor that FEMA can use to leave a message for the applicant. Note: Include extension number (if available).
8. Enter the full physical street address at which the damage occurred. Do not enter a P.O. or general delivery address.
9. Enter the applicant's mailing address. It may or may not be the same as the Damaged Property Address or where the applicant is now living. The Mailing Address may be a post office or general delivery address. If it is the same as the damaged property address, check the box for the same.
10. Check Cause of Damage (more than one cause may be checked). Other causes of damage may include explosion, drought, and riot. If more than the home was damaged (e.g., auto was flooded), please describe in the Comments section in item no. 30.
11. If the applicant has damage to the home (e.g., electrical, heating, floors, walls, ceilings, and foundation), check Yes. If home damage is unknown, check Unknown.
12. If the applicant had Personal Property Damage, e.g., appliances, clothing, and/or furniture, check Yes.
13. If the applicant's utilities are not working (out), check "Yes." Utilities may include sewer, water, gas, electricity, and/or heating.
14. Check the current Location where the applicant is living.
15. Check the type of residence that was damaged (e.g., Travel Trailer, Mobile Home, House-Single/Duplex, etc.). Other may include, for example, homeless or RV.)
16. If the person lived in the home more than six months of the year, or the applicant lists it as the address of his/her Federal Tax Return, or the applicant files a homestead exemption, or the applicant uses it as a voter registration address, check "Yes."
17. If the applicant is named on the deed, or the applicant maintains the home and pays the taxes but pays no rent, or the applicant has lifetime occupancy rights while not holding legal title to the home, check Own. Check "Rent" if the applicant does not meet any of the above ownership criteria, even if the applicant pays no rent.
18. If the home is Accessible after the disaster, check "Yes." Inaccessible may include disruption or destruction of transportation routes or other obstructions that prevent the applicant from gaining entry to the damaged home. If the applicant is unable to enter the home, determine if it's Due to the Disaster, or Due to Mandatory Evacuation and check appropriately.
19. List the type of insurance that the applicant held at the time of the disaster for the home and/or personal property, including but not limited to sewer backup, earthquake. Include the name of the insurance company. If no insurance, check I have no insurance for my home or personal property.
20. If the applicant incurred a Medical, Dental, Funeral, and/or Moving Storage Expense related to the disaster, check "Yes." Under Insurance company, provide the name of applicant's insurance company if they had insurance for that expense.
21. Enter all vehicles for the household (regardless of condition) and their year, make, and model. If the applicant or one of the applicant's dependents owns a vehicle(s) that was damaged by the disaster, check "Yes." Also, check "Yes" for the vehicles that are drivable. Check "Yes" if the listed vehicle(s) has Comprehensive and/or Liability Insurance, and if the vehicle(s) is registered. Enter the name of the insurance company if applicant has insurance. If more space is needed, use the space in item #29.
22. If the applicant had Other Expenses, check the types of expenses that apply (i.e., generator, chainsaw).
23. If the applicant has Emergency Needs (e.g., food, clothing, shelter), check the appropriate box for type of need.
24. Question relates to special needs. The Americans with Disabilities Act (ADA) defines a disability as "a physical or mental impairment that substantially limits one or more of the major life activities of such individual." 42 USC 12102(2)(A). If the registrant or household member has such a disability and was affected by the disaster, please mark all of the areas of disability that apply.
25. List information for the applicant and all other persons/dependents who consider the home to be their primary residence at the time of the disaster, whether or not they are related to the applicant. It is important that the applicant's and co-applicant's SSN is included. Answer if they are a dependent or not.
26. LOST WORK? If the applicant or a member of the applicant's household lost work or became unemployed as a result of the disaster for which they will not be compensated, check "Yes." An example is, if the family breadwinner was incapacitated or killed due to the disaster.
SELF EMPLOYMENT IS PRIMARY INCOME? Check appropriately.
OWNS/REPRESENTS BUSINESS OR RENTAL PROPERTY? Check appropriately.
27. Enter the number of claimed dependents as listed on the applicant's Federal Tax Return.
28. Enter the combined family pre-disaster gross income. (This is the amount of income before any deductions, and may include money from employment, Social Security, retirement, welfare, child support, stocks, interest, annuities, and savings or assistance from family and friends. It does not include food stamps or HUD Section 8 assistance.) Check the appropriate frequency of pay (weekly, bi-weekly, monthly, semi-monthly, quarterly, or yearly). If income refused, check appropriate box.
29. If the applicant would like FEMA to automatically transfer assistance into their checking or savings account, check "Yes" next to Electronic Funds Transfer. Enter the name of the applicant's financial institution. Enter the applicant's 9-digit routing no. (The routing no. is the 9-digit number that appears in the lower left hand corner of the check.) Indicate the applicant's account type by marking the Checking or Savings box. Enter the applicant's account no. (The account number can be found at the center bottom of a check immediately after the routing number, or can be found on a savings or checking account statement.) NOTE: Applicant name must be on the account.
30. If applicable, enter Social Security Administration's Change of Address Request
31. Enter any additional comments as necessary.
32. Enter name of the FEMA representative filling out form.

PRIVACY STATEMENT

The Robert T. Stafford Disaster Relief and Emergency Assistance Act, 42 U.S.C. §§ 5121-5206. Executive Order 12149, as amended, and Title IV of The Personal Responsibility and Work Opportunity Reconciliation Act of 1996, 9 U.S.C. §§ 1601 et seq., authorizing the collection of this information. The primary use of this information is to determine your eligibility to receive FEMA disaster assistance. Disclosure of this information may be made: upon written request, to federal and state agencies providing disaster assistance, as well as to local governments or voluntary agencies from which you are seeking assistance, so that assistance efforts or benefits are not duplicated; to agencies, organizations and institutions as necessary for FEMA to obtain information from them in making eligibility determinations; to federal, state, and local government agencies to promote hazard mitigation planning and enforcement; to law enforcement agencies or professional organization where there may be violation or potential violation of law; to a federal, state, or local agency we request information relevant to an Agency decision concerning issuance of a grant or other benefit, or in certain circumstances when a Federal agency requests such information for a similar purpose from us; to a Congressional office in response to an inquiry made at the request of the individual; to the Office of Management and Budget (OMB) in relation to private relief legislation under OMB circular A-19; and to the National Archives and Records Administration in records management inspection conducted under the authority of 44 U.S.C. §§ 2904 and 2906. Your Social Security number is solicited during registration pursuant to the Debt Collection Improvement Act of 1996, 31 U.S.C. §§ 3326(d) and 7701(c)(1). Furnishing the social security number, as well as other information, is voluntary, but failure to do so may delay or prevent provisions of disaster assistance.

PAPERWORK BURDEN DISCLOSURE NOTICE

Public reporting burden for this form is estimated to average 18 minutes per response. The burden estimate includes the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and submitting the form. You are not required to respond to this collection of information unless a valid OMB control number is displayed in the upper right corner of this form. Send comments regarding the accuracy of the burden estimate and any suggestions for reducing the burden to: Information Collections Management, Department of Homeland Security, Federal Emergency Management Agency, 500 C Street SW, Washington, DC 20472. Paperwork Reduction Project (1660-0002).

NOTE: DO NOT SEND YOUR COMPLETED FORM TO THIS ADDRESS.

The Tele-Registration recording informs the respondent at the beginning of the registration intake of the Privacy Act and Paperwork Reduction Act (PRA) burden disclosure information.

It is not necessary to complete grayed fields.