Privacy Impact Assessment
for the

Disaster Assistance Improvement Program (DAIP)

DHS/FEMA/PIA-012(a)

November 16, 2012

<u>Contact Point</u>
Karole Johns
Disaster Assistance Improvement Program
Federal Emergency Management Agency
(540) 686-3211

<u>Reviewing Official</u>
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Federal Emergency Management Agency (FEMA), Office of Response & Recovery (OR&R), Recovery Directorate, National Processing Service Center (NPSC) Operations Branch sponsors and funds the Disaster Assistance Improvement Program (DAIP). In accordance with Executive Order 13411 “Improving Assistance for Disaster Victims,” DAIP developed the Disaster Assistance Center (DAC) system. As a part of DAIP, DAC maintains disaster survivor application and registration information collected through various media including: (1) DAIP paper forms (attached at Appendix A), (2) the www.disasterassistance.gov website, (3) the http://m.fema.gov mobile website, and (4) via telephone. DAIP/DAC shares the information with the National Emergency Management Information System (NEMIS) – Individual Assistance (IA)[1] module to facilitate eligibility determinations and with other federal, tribal, state, local, and non-profit agencies/organizations that also service disaster survivors. FEMA is conducting this Privacy Impact Assessment (PIA) because DAIP/DAC collects, uses, maintains, retrieves, and disseminates personally identifiable information (PII) of disaster survivors who either request IA benefits from FEMA or whom FEMA may refer to its partners.

Overview

FEMA OR&R, Recovery Directorate, NPSC Operations Branch sponsors, funds and manages DAIP/DAC, to meet the mandate of Executive Order 13411, which requires the federal government to simplify the process of identifying survivors of a terrorist attack, natural disaster, or other incident that is the subject of an emergency or major disaster declaration under the Stafford Act and their applications for disaster assistance. FEMA developed DisasterAssistance.gov and DAC to address this requirement. Through this website, FEMA consolidates disaster assistance information from seventeen federal government agencies and provides disaster survivors with a mechanism to access and apply for disaster assistance through the collaborative efforts of federal, tribal, state, local, and non-profit partners. Through the DisasterAssistance.gov website FEMA offers disaster survivors a multitude of services including:

- a comprehensive, one-stop, online application intake capability that meets the minimum initial applicant information collection requirements of all federal disaster assistance providers;
- immediate, secure, targeted, horizontal exchange of collected applicant information with all appropriate federal disaster assistance provider organizations;

[1] *See* DHS/FEMA/PIA-027 – National Emergency Management Information System-Individual Assistance (NEMIS-IA) Web-based and Client-based Modules, *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_fema_nemis_ia_20120629.pdf.

- real or near-real time verification of every applicant's identity and an automatic referral mechanism for those applicants whose identity cannot be verified;
- automated system-to-system updating of new/changed applicant information; and
- the capability for applicants to review the progress/status of applications for all federal disaster assistance providers.

DAIP/DAC is the IT system that supports the registration processes associated with DisasterAssistance.gov, and as such facilitates the information collection, sharing, and processing activities necessary to provide IA to disaster survivors. Examples of transactions depicting these activities are included below.

Help Finding Assistance and Creating a Disaster Assistance Registration/Application

Following a presidentially-declared disaster that is designated as eligible for IA benefits, a survivor affected by the disaster who wants to apply for assistance online navigates to the DisasterAssistance.gov portal using an Internet web browser or browser-enabled smartphone. At DisasterAssistance.gov, survivors have three options to choose from: 1) "Find Assistance;" 2) "Apply for Assistance;" or 3) "Check Your Application Status." If the survivor needs DAIP's help to determine the types of disaster assistance for which they might be eligible, he or she may click a button marked "Take Questionnaire," and complete an online survey hosted by the U.S. Department of Labor (DOL) that is composed of questions about assistance needs, damage types, citizenship status, and the location of the damaged property, among others, by clicking a series of checkboxes. DAIP does not collect name or any other PII from the disaster survivor through this survey. Based upon pre-defined business rules that participating programs provide, DisasterAssistance.gov returns a list of assistance programs for which the survivor may be eligible, along with program and contact information about other forms of assistance that may be available to aid the survivor.

Either after being pre-screened for eligibility, or directly upon clicking the "Apply for Assistance" link on the website using a personal computer or smartphone, the survivor may choose to apply for disaster assistance. To do so, the survivor is taken to a web page clearly denoted as the "Disaster Assistance Center," at which point he or she proceeds by clicking a button labeled "start." At this point, and any point through the pre-screening and registration processes, the survivor has the option to exit by clicking a "Delete This Registration" button. Also at this point, after clicking the "Start" button, DAIP provides the survivor with both the Paperwork Reduction Act, and after another click of the "next" button, the Privacy Act statement (attached at Appendix C). To proceed with the identity verification and application processes, the applicant must click a check-box accepting the Privacy Act statement.

To begin the registration process, the survivor provides DAIP with PII such as name, address, social security number (SSN), and date of birth (DOB). DAIP then shares this information with a third-party identity proofing (IdP) service that conducts an identity verification. After identity verification, the survivor is presented with an application form for the disaster assistance programs for which the individual may be eligible. The survivor only completes the application once, and the application information is used to apply for assistance from multiple federal programs. To minimize the amount of information collected from survivors, DAIP/DAC provides the survivor with only those fields from the selected disaster assistance applications that he or she must complete in order to qualify for assistance from programs linked to the applicant from the pre-screening questionnaire.

When the survivor submits the single application, DAIP/DAC routes the information accordingly. If the survivor is requesting assistance from a FEMA program, information is passed to the shared NEMIS database, in which it is shared with the NEMIS-IA system, which processes the information and returns status updates. For other participating department and agency programs, DAC routes survivor information to a secure data exchange point to provide the applicant information with external partner agencies.[2] The DAC application notifies applicable departments and agencies that an application has been submitted for evaluation. Participating departments and agencies receive survivor information, immediately or at a time of their choosing, to determine survivor eligibility and continue processing the application. Participating departments and agencies are also able to determine what other assistance the survivor has requested using this application form, which assists in identifying and reducing potential duplication of benefits. The DAC application also routes agreed-upon data sets of survivor information to the Enterprise Data Warehouse[3] for subsequent processing and reporting.

Survivors retain the option to apply for assistance via telephone through existing NPSC call centers. NPSC call center protocols and procedures have been retooled to reflect the universal application format contained herein, ensuring that a survivor applying by telephone need only submit a single application for assistance.

DAC Account Creation

DAIP uses a third-party identity proofing (IdP) service to verify the identity of potential DAC users during the account creation process prior to the disaster survivor's completion and submission of an application for assistance. If the survivor choses to authenticate after submitting an application for assistance, he can do so at any time after the initial application has been submitted.

[2] The data exchange point is an instance of a Service Oriented Architecture application. The data exchange point transfers information back and forth securely between FEMA and selected partners to facilitate requests for assistance.

[3] *See* DHS/FEMA/PIA-026 – Operational Data Store and Enterprise Data Warehouse, *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_fema_ods_edw_20120629.pdf.

Identity Verification Process

Upon visiting www.disasterassistance.gov and clicking the link to begin the registration process, but after receiving the PRA and Privacy Act statements, DAIP requires the applicant to provide his or her title (Mr. or Ms.), first and last name, SSN, and DOB. Applicants may also provide middle initial and email address, but both are optional. DAIP then sends the following four data elements, first name, last name, SSN, and DOB, via a secure web service to the IdP. The IdP queries its database of public records to determine whether a person with these characteristics, including SSN exists and provides a Yes/No status flag to DAIP. DAIP receives no other information from the IdP, and under the DAIP contract with the IdP, this information may not be used by the IdP for any other purpose. This initial process allows the survivor to apply for assistance through the call center, but does not allow the survivor to conduct status inquiries or updates. Based on the determination, the system either allows the applicant to proceed through the DAC account creation process or informs them that the information does not match and directs them to contact the NPSC call center.

Identity Authentication Process

At the end of the disaster assistance application process, applicants are encouraged to create an authenticated DAC user account to enable access to system's self-service features, including status inquiries and applicant information updates. If the survivor does not create an authenticated user account at the end of the initial disaster assistance registration process, the survivor will need to create one when he or she returns to the site at a later time to be able to check status inquiries or provide updated information. Alternativley, FEMA will send follow up information via postal mail. When creating a DAC-authenticated account, DAIP sends the same four data elements presented for identity verification to the IdP, which uses these four elements to develop a four question quiz. The four question quiz is against out-of-wallet[4] information from the IdP of public records (e.g., the quiz might ask the applicant to identify what street they have lived on in the past ten years, given a list of choices). In order to create a DAC-authenticated account online, the applicant must answer at least three out of four multiple choice questions correctly. If an applicant fails the authentication quiz, the IdP generates new questions for a subsequent authentication attempt. Applicants may fail the identity authentication questions three times before DAIP prevents them from creating an online account. IdP returns a Yes/No decision on identity authentication to DAIP, and does not provide specific information on the quiz answers or scoring related to an individual. The IdP does provide aggregate information related to pass/fail rates and for billing purposes.

After authentication, DAIP sends a PIN code to the survivor via e-mail or United States Postal Service (USPS) mail. Once received, the survivor is then able to login to his or her

[4] Out-of- wallet data is generally considered data that is not available if an individual's wallet were stolen.

account with his or her username, password, and PIN code to view a list of disaster assistance applications under evaluation and to see the status of each, or to make any necessary changes to his or her application.

If an applicant fails the identity verification and/or identity authentication checks during any part of the application process, they can still apply or obtain status through the NPSC call center.

Checking the Status of Your Complete Disaster Assistance Application

Applicants may return to DisasterAssistance.gov to check on the status of their disaster assistance application. Upon accessing the site, applicants click on "Check Your Application Status" button to receive the login screen to access their account. At the login screen, the survivor logs in to their DAC account with his or her username, password, and PIN code to view a list of disaster assistance applications under evaluation and to see the status of each, or to make any necessary changes to his or her application. The DAC presents the applicant with status information received from programs to which applications were referred, such as the NEMIS-IA system. Based upon the respective business rules of NEMIS-IA and other participating programs, the programs push application status information through a secure method to the DAC account. When a survivor accesses his or her account, the DAC application receives updated status information from the data exchange point. Likewise, the DAC application pushes updated application information to the data exchange point, where those programs processing the application receive the information and update the application. Once updated, the DAC application notifies the appropriate programs that updates are available.

Customer Satisfaction Analytics

FEMA has contracted with a third-party vendor to collect and report data on disaster assistance applicants' satisfaction with FEMA's DisasterAssistance.gov website.[5] FEMA leverages the customer satisfaction service to gather customer input from an online survey. Respondents choosing to take the survey may rate overall satisfaction and different aspects of the Web experience (e.g., search, usability) through open-ended or multi-choice custom questions. The survey can usually be completed in just a few minutes. FEMA receives reporting and analysis on a regular basis and uses this information to modify its website to better meet the needs of disaster survivors seeking assistance from FEMA.

Applicants who have completed the registration process and successfully created a DAC account may return to the site to check the status of their application. Upon logging in to the

[5] Further discussion related to DHS' use of social networking applications can be found in the DHS/ALL/PIA-031 Use of Social Networking Interactions and Applications Communications/Outreach/Public Dialogue found at www.dhs.gov/privacy.

status inquiry portion of the website, a random sample of these visitors may be presented with a request to participate in the ForeSee survey. The size of the sample is determined based on the percentage of visitors the DAIP wishes to survey; this percentage can easily be changed to increase or decrease the size of the sample. If the user chooses to take the survey, a new window will open in the background so he or she can take the survey after they exit from Applicant Inquiry. No session information or PII is captured. Individuals can opt out of taking the survey by closing the request window or selecting "No Thanks." Opting out does not in any way impact the processing of the individual's disaster assistance application. Individuals who decline the survey will have access to the identical information and resources on the website as those who choose to take survey.

Online Sharing Tools

To promote the ease of sharing of disaster assistance information via social media, FEMA uses a social bookmarking and sharing widget that allows users to share articles, web pages, and other web content with their social media circle on Facebook, Twitter, or other social media platforms.[6] Upon visiting DisasterAssistance.gov, if a survivor decides he or she wants to share information he or she finds there (e.g., instructions on applying for assistance, FEMA's contact information, etc.) on a social media site, he or she may do so by clicking on the "AddThis" button on the website. The application programming interface (API) will capture the uniform resource locator (URL) for the DisasterAsssitance.gov web page and pass it to the social media site chosen by the visitor, allowing the URL to be posted on the visitor's social media site/page.

Through this process, the online sharing tools collects information about the user's browser type, operating system and chosen social media platform and aggregates this information for FEMA OR&R, NPSC Operations Branch to review. The information that FEMA receives from the AddThis widget does not contain PII, only an aggregate number of users. The use of AddThis is strictly voluntary. Disaster assistance applicants may opt out by simply choosing not to use the widget to share information. The use of the tool on the part of a visitor to DisasterAssistance.gov does not in any way impact FEMA's provision of assistance or service to the website visitor.

Google Analytics

[6] Further discussion related to DHS' use of social networking applications can be found in the DHS/ALL/PIA-031 Use of Social Networking Interactions and Applications Communications/Outreach/Public Dialogue found at www.dhs.gov/privacy.

Consistent with other websites at DHS, FEMA's DisasterAssistance.gov website uses Google Analytics to help analyze how users use the site.[7] Google Analytics is a free, external, third-party hosted, website analytics solution that generates robust information about the interactions of public-facing website visitors with FEMA. The tool uses "cookies," which are text files placed on an individual's computer, to collect standard internet log information and visitor behavior information. Google Analytics uses first-party cookies to track visitor interactions. The information generated by the cookie about the use of the website (including IP address) is transmitted to Google. This information is then used to evaluate visitors' use of the website and to compile statistical reports on website activity for DAIP. Google Analytics must collect the full IP Address, which Google will then mask prior to use and storage, and proceed with providing the Department non-identifiable aggregated information in the form of custom reports.

FEMA does not permit third parties operating on DisasterAssistance.gov to use statistical analytics tools to track or to collect any PII from visitors to our site. Google will not associate a visitor's IP address with any other data held by Google. Neither FEMA nor Google will link, or seek to link, an IP address with the identity of a computer user. FEMA will not associate any data gathered from this site with any PII from any source, unless you explicitly submit that information via a fill-in form on our website.

Address Correction

DAIP uses a third party service product to confirm mailing and damaged dwelling addresses submitted by disaster survivors via DisasterAssistance.gov. The third party provides compact discs of address information to DAIP quarterly, and DAIP uploads the information to its servers to ensure that the product is available to users. If a survivor provides an address that is not recognized when compared with the address database, the applicant is asked for a correction. If DisasterAssistance.gov determines the need for address correction, it presents the corrected address from the address database to the applicant for acceptance, or the applicant may override with manual entry. This process ensures a high rate of accuracy for the address information DAIP/DAC collects and that the information provided is associated with a known address.

Sharing Disaster Assistance Application Data with Partner Agencies

As DAIP/DAC and DisasterAssistance.gov were designed to be a single information collection point for multiple sources of assistance, DAIP routinely shares disaster assistance registration information with federal, state, local, tribal, and non-profit partners, as described in greater detail in Section 6 of this PIA. Applicant data may be shared with one or more partner agencies, depending on eligibility criteria and applicant interest in other forms of assistance.

[7] For additional information on DHS's use of the Google Anayltics tool, *see*: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhs_ga.pdf

Additionally, as noted above, DAIP may receive from its partner's status updates pertaining to individuals' disaster assistance applications, such as with Small Business Administration.

All information exchanged using the DAC application is over a secure connection and complies with the routine uses described in the DHS/FEMA-008 Disaster Recovery Assistance Files System of Records, 74 FR 48763, September 24, 2009.[8] Disaster recovery assistance files, such as those for FEMA's IA programs that are contained in DAIP/DAC, are retained for six (6) years and three (3) months in accordance with NARA Authority N1-311-86-1, items 4C10a and 4C10b, also described in the DHS/FEMA-008 Disaster Recovery Assistance Files System of Records Notice.

The primary privacy risks associated with DAIP/DAC include the possible inaccuracy of the identity verification and the possible erroneous disclosure of DAIP/DAC PII to third party vendors or external partner agencies. In order to mitigate the risk of an inaccurate failure, DAIP/DAC set up a manual review process for applicants who have received a "fail" flag. In order to mitigate the risk of inaccurate passing, DAIP has agreements in place with the third party IdP that guarantees the accuracy of the data. DAIP conducts routine reviews of the accuracy of this data. To mitigate the risk of erroneous external disclosure, DAIP limits sharing the information in DAIP/DAC outside of DHS pursuant to only the routine uses found in the DHS/FEMA-008 Disaster Recovery Assistance Files System of Records, 74 FR 48763, September 24, 2009, and only using appropriate security controls as outlined in the Interconnection Security Agreements (ISA) approved for each agency integration. In addition, DAIP restricts the access of its partner agencies to only that information relevant to their respective programs, and only to those individuals with a "need to know" for the specific data.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

Section 408 of the Robert T. Stafford Disaster Relief and Emergency Act, as amended, 42 U.S.C. § 5174, allows the President to provide financial assistance to individuals and households in the state which, as a direct result of a major disaster, have necessary expenses and serious needs that they are unable to meet through other means.

Section 312 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended, 42 U.S.C. § 5155, prohibits persons, business concerns, and other entities from receiving benefits for a loss that would duplicate financial assistance under other programs, from insurance, or from any other source.

[8] *See*, http://www.gpo.gov/fdsys/pkg/FR-2009-09-24/html/E9-23015.htm.

In addition to the above the following are relevant authorities:

- The Clinger Cohen Act, 40 U.S.C. § 11303, guidance for multiagency investments, and 40 U.S.C. § 11318, guidance for interagency support;
- Section 401 of the Personal Responsibility and Work Opportunity Reconciliation Act of 1996, 8 U.S.C. § 1611;
- The Debt Collection Improvement Act of 1996, 31 U.S.C. § 3711(g);
- The Economy Act, 31 U.S.C. § 1535;
- The Paperwork Reduction Act, as amended, 44 U.S.C. § 3501, et. seq.;
- 44 C.F.R. §§ 206.110-119, Federal assistance to individuals and households;
- 44 C.F.R. § 206.191, Duplication of benefits; and
- Executive Order No. 13411, Improving Assistance for Disaster Victims, August 29, 2006, 71 FR 52729 (Sep. 6, 2006), requires Federal Agencies to improve disaster assistance to the public by providing centralized access to all federally-funded disaster assistance programs.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The information collected by DAIP/DAC is covered by the DHS/FEMA-008 Disaster Recovery Assistance Files System of Records, 74 FR 48763, September 24, 2009.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

DAIP/DAC is covered by a System Security Plan (SSP) for the project dated May 23, 2011. The system has been granted an Authority To Operate (ATO) on November 20, 2010, which expires on November 20, 2012. An Authority to Proceed (ATP) was granted on August 15, 2012, in conjunction with the implementation of the DAIP instance at Data Center 2. The ATP expires on November 16, 2012, at which time a new ATO is expected to be issued. DAIP will revise and reissue the SSP when the revision process has been completed.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

FEMA retains IA program files in order to administer assistance actions and to evaluate the progress of the program among other authorized uses. FEMA will retire to inactive storage and destroy records pertaining to IA, except those relating to temporary housing, when six (6) years and three (3) months old in accordance with NARA Authority N1-311-86-1, item 4C10a. FEMA will destroy records pertaining to temporary housing three (3) years after close of the operation in accordance with NARA Authority N1-311-86-1, item 4C10b. Closeout occurs when the disaster contract is terminated. Records pertaining to the Individuals and Households Program (IHP) will retire to the Federal Records Center one (1) year after closeout and will be destroyed three (3) years after closeout.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The information that DAIP/DAC collects, uses, maintains, retrieves, and disseminates is collected through Office of Management and Budget (OMB) Control No. 1660-0002, "Disaster Assistance Registration," (expires August 31, 2013); and OMB Control No. 1660-0061, "Federal Assistance to Individuals and Households Program," (expires October 31, 2014).

See Appendix A for a list of approved forms related to each collection.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

DAIP/DAC requires disaster survivors, applying for assistance via the Web Portal (desktop computer, tablet computer or smartphone with browser), telephone, or paper form, to provide the following information:

- Applicant Information:
    - Name (Prefix, First Name, Middle Initial, Last Name),
    - Language Spoken,
    - DOB,
    - SSN, and
    - Email Address,
- Contact Information:
    - Mailing Address (Street, Appt/Lot, City, State, Zip, County/Parish/Municipality (county data is not collected on paper Form 009-0-1)),
    - Current Phone Number and Notes,

  - Alternate Phone Number and Notes,
  - Cell Phone Number,
- Damaged Dwelling Information:
  - Damaged Property Address (Street, Appt/Lot, City, State, Zip, County/Parish/Municipality),
  - Damage Dwelling Phone Number,
  - Alternate Damaged Phone Number,
  - Cause of Damage,
  - Type of Damage Sustained (Home, Personal Property, Utilities Out),
  - Residence Type,
  - Is it a Primary Residence? (Yes/No),
  - Own or Rent,
  - Is Home Accessible? (Mandatory Evacuation (Yes/No), Due to Disaster (Yes/No)),
- Home/Personal Property Insurance (Type, Insurance Company Name);
- Disaster Related Expenses (Medical, Dental, Funeral, Insurance Companies);
- Disaster Related Vehicle Damage:
  - Vehicle Information (Year, Make, Model),
  - Extent of Damage (Damaged (Yes/No), Drivable (Yes/No)),
  - Vehicle Insurance (Comprehensive, Liability, Insurance Company Name),
  - Vehicle Registered? (Yes/No),
- Other Expenses (Chainsaw, Wet/Dry Vacuum, Generator, Dehumidifier);
- Emergency Needs (Food, Clothing, Shelter);
- Special Needs (Mobility, Mental, Hearing, Vision, Other Care);
- Occupant Information (for all occupants at time of disaster):
  - Name (First Name, Middle Initial, Last Name),
  - SSN,
  - Age,

  - Relationship to Applicant,
  - Dependent? (Yes/No),
- Business Damage:
  - Self-Employment is Primary Income? (Yes/No),
  - Business or Rental Property Affected? (Yes/No),
- Number of Dependents Claimed;
- Combined Family Pre-Disaster Gross Income (By Period);
- Authorization for Electronic Funds Transfer of Benefits:
  - Institution Name,
  - Account Type,
  - Account Number and Routing Number,
- Authorization for Postal or Email Notification;
- Authorization for Social Security Change of Address;
- Comments from the Applicant;
- FEMA Representative Name (if filling out the form);

Information Provided by Third Parties

- "Pass/Fail" flag (for identify verification provided by third-party identity verification service); and
- Third party address database (for address correction).

Information Generated by NEMIS-IA During Processing and Returned to DAIP/DAC

- FEMA Disaster Number (generated by FEMA; provided to survivors via NPSCs, Disaster Recovery Centers, etc.);
- Application Status ("In-Process," "Submitted," or "Approved");
- Housing Inspection Required (Y/N);
- Priority of Assistance;
- Type of Assistance being considered; and

- Time Stamps.

DAIP/DAC Information Supplied by Partner Agencies

- Change of Address Status Code (from the U.S. Social Security Administration);
- Disaster Loan Event Status Code (Rejected, Approved, Declined, Verified, Cancelled) (from the U.S. Small Business Administration);
- Pre-registration Questionnaire Information (from the U.S. Department of Labor);
- Pre-registration Questionnaire Session ID (from the U.S. Department of Labor); and
- Food for Florida Pre-registration ID and Application Status (from the State of Florida).

2.2 What are the sources of the information and how is the information collected for the project?

The sources of information in DAIP/DAC are the IA disaster applicants, external partner agencies, DAIP's third-party IdP service and DAIP's third-party address verification product.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

Yes. DAIP secures identity verification characteristics and authentication services from the IdP. DAIP collects full name, address, SSN, and DOB from disaster survivors and sends an identity verification query via a secure web service to the IdP, which then performs a query of its database of public records to determine if a person with these characteristics exists and returns a yes/no status. DAIP authenticates users by sending the same data to the IdP, which then sends a four question quiz to the applicant to answer. The quiz and answers are then used to authenticate returning users. DAIP receives no other information from the IdP, and under the DAIP contract with the IdP, this information may not be used by the IdP any other purpose.

DAIP also compares applicant addresses against a third-party address database. It presents the known address to the applicant for review, acceptance or modification.

2.4 Discuss how accuracy of the data is ensured.

DAIP/DAC assumes the accuracy of the information that it receives directly from individual disaster assistance applicants; however, DAIP does take steps to ensure the accuracy of the data.

First, DAIP mails every applicant seeking IA a hard copy printout of his or her original DAIP/DAC application, which provides an opportunity to identify any errors in the original application submitted to DAIP. Second, applicants have the opportunity to speak with a FEMA case worker at a NPSC location to correct any deficiencies in the applicant's DAIP/DAC data. In addition, for applicants who choose to use the telephone application process and provide information to the tele-registrar, who in turn will enter the data into the system, the address database provides screen pre-population data to the tele-registrars to help ensure data accuracy.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a privacy risk that DAIP/DAC could maintain inaccurate information from disaster assistance applicants. This might cause the individual to receive no assistance or less assistance than he or she is qualified to receive.

Mitigation: DAIP mitigates this privacy risk by sending each applicant a hard copy printout of his or her application, thus providing the applicant with knowledge of any errors that may exist within it. In addition, DAIP offers applicants multiple methods of correcting any discrepancy in their data so that it will properly process their applications, such as making edits to their data via www.disasterassistance.gov or contacting a NPSC representative via DAIP's toll-free assistance hotline.

Privacy Risk: There is a privacy risk that the identity verification "pass/fail" flag inaccurately fails or passes an individual.

Mitigation: DAIP mitigates this privacy risk by setting up a manual review process for applicants who have received a "fail" flag. In order to mitigate the risk of inaccurate passing, DAIP has agreements with IdP that guarantees the accuracy of the data. DAIP conducts routine reviews of the accuracy of data from the IdP. If IdP inaccurately passes an applicant, the applicant is not able to access any status information without going through the identity authentication process.

Privacy Risk: There is a privacy risk that the identity authentication process will inaccurately fail an individual.

Mitigation: DAIP mitigates the privacy risk related to identity authentication by setting up a manual review process, similar to that for identity verification, for applicants who have received a "fail" flag. In order to mitigate the risk of inaccurate passing, DAIP has agreements with IdP that guarantees the accuracy of the data. DAIP conducts routine reviews of the accuracy of data from the IdP.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

DAIP/DAC collects and shares the information listed in Section 2.1 to identify disaster survivors and to determine their eligibility for assistance from DAIP and its participating federal, tribal, state, local, and non-profit agency/organization partners. It uses the information to communicate the status of assistance with applicants. In addition, selected elements of applicant information (Name, SSN, Address, and DOB) are shared with the IdP to verify and authenticate an applicant's identity. DAIP receives no other information from the IdP, and under the DAIP contract with the IdP, this information may not be used by the IdP any other purpose.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No, the project does not use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or anomaly.

3.3 Are there other components with assigned roles and responsibilities within the system?

No, there are no other DHS components with assigned roles and responsibilities within DAIP/DAC.

3.4 <u>Privacy Impact Analysis</u>: Related to the Uses of Information

<u>Privacy Risk</u>: A privacy risk associated with this system includes DAIP or its partners using the information for purposes other than that for which it was originally collected.

<u>Mitigation</u>: DAIP mitigates this risk in several ways. First, DAIP limits its data collection in DAIP/DAC to only that which is required to process disaster assistance applications, so there is no extraneous data stored or shared with its partners. Second, DAIP also limits access to DAIP/DAC to authorized users whose access is based on their roles and responsibilities and who have signed Rules of Behavior documentation. Third, DAIP has a contract with the IdP that limits the use of the information provided by survivors to only those uses associated with the DAIP identity verification and authentication processs. Last, DAIP/DAC data is shared and used by the project and external partners based on the Interconnection Security Agreements (ISA) and Interface Control Documents (ICD).

DAIP/DAC only provides each partner agency with authorized data using data exchange protocols agreed to by the project and the partners.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

DAIP provides notice of its collection of information in DAIP/DAC through many different media. DAIP provides a Privacy Act Statement (attached at Appendix C) on Form 009-0-1 and its variations (attached Appendix A), as well as its other IA program forms. DAIP also provides this Privacy Act Statement to applicants via http://www.disasterassistance.gov/ prior to collecting information for disaster assistance registrations. Survivors applying via the internet must accept the Privacy Act Statement before DAIP/DAC will allow them to advance to the point where their data is collected. In addition, NPSC case workers provide a Privacy Act Statement to applicants verbally prior to collecting any disaster assistance registration information. Last, this PIA and DHS/FEMA-008 Disaster Recovery Assistance Files System of Records, 74 FR 48763, September 24, 2009, provide notice of DAIP's collection of information for IA programs.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

DAIP provides disaster assistance applicants the opportunity to consent or decline to provide information for a disaster assistance registration/application prior to the information being processed by DAIP/DAC. DAIP provides notice of the information collection, including the consequences to the individual of failing to provide the information requested in the disaster application/registration process through several media, as described in Section 4.1. An individual may opt-out by simply declining to provide the information, or specifically regarding DisasterAssistance.gov, by clicking the "Delete This Registration" button at any time in the online process; however, once the individual provides information to DAIP during the application/registration process, that information will be processed by DAIP/DAC.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a privacy risk that the individual survivors applying for assistance via DAIP/DAC will not receive notice at the time their information is collected.

Mitigation: DAIP mitigates this privacy risk by providing notice of its collection of information to facilitate the provision of its IA programs in several ways including through

Privacy Act Statements on its paper forms, web, and mobile sites, and a verbal Privacy Act Statement provided by NPSC staff that provide telephone assistance to applicants. In addition, disaster survivors using the www.disasterassistance.gov website to apply for assistance must electronically accept the Privacy Act Statement before DAIP will collect their information as part of the application process. Last, this PIA and DHS/FEMA-008 Disaster Recovery Assistance Files System of Records, 74 FR 48763, September 24, 2009, provide notice of DAIP's collection of information for IA programs.

Section 5.0 Data Retention by the project

5.1 Explain how long and for what reason the information is retained.

DAIP retains application/registration information for its disaster assistance programs in accordance with NARA Authority N1-311-86-1, item 4C10a, and as described in DHS/FEMA-008 Disaster Recovery Assistance Files System of Records, 74 FR 48763, September 24, 2009. The information is retained for six (6) years and three (3) months, which allows time for DAIP to resolve any appeals that an applicant may pursue regarding his or her eligibility determination.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a privacy risk that DAIP/DAC will retain the information longer than necessary.

Mitigation: DAIP mitigates this risk by minimizing the time it keeps the data, in line with the mission of its disaster assistance programs, and by allowing for appeals. In addition, DAIP leverages training and documentation, such as Standard Operating Procedures to inform DAIP users and operators of proper record retention standards.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Yes. To meet the ends of Executive Order 13411, "Improving Assistance for Disaster Victims," DAIP shares selected data with other federal, tribal, state, local, and non-profit agencies/organizations in accordance with the routine uses published in DHS/FEMA-008 Disaster Recovery Assistance Files System of Records, 74 FR 48763, September 24, 2009. FEMA has shared information via one-time routine use written requests as well as through memorialized agreements allowing for ongoing transmission of information. Formalized agreements are in place with those agencies/organizations with which the project currently shares data, as described below:

- Small Business Administration (SBA)

  Under routine use R, pertaining to computer matching agreements undertaken to prohibit a duplication of benefits, DAIP shares disaster applicant information for applicants who exceed the SBA provided income threshold with the SBA Disaster Credit Management System (DCMS) for low-interest loan consideration. Once a loan determination is made, SBA will pass status information back to DAIP. DAIP may provide additional assistance based on SBA's determination.

- Social Security Administration (SSA)
  - Under routine use Q, pertaining to the updating of records, DAIP shares disaster-related change of address information including effective date to SSA so that disaster survivors who are also Social Security beneficiaries may have their benefits checks sent to their temporary or new residence following a major or catastrophic disaster situation. Only disaster survivors who have registered for IA and are existing Social Security beneficiaries will be allowed to update their change of address via DiasterAssistance.gov or its supporting call centers.
- Department of Education (DoED)
  - Under routine use Q, DAIP shares information with DoED. DAC can redirect an applicant so that he or she can access their existing DoED National Student Loan Data System (NSLDS) account. This transaction posts the DAC user's data to the target landing URL provided by DoED. DoED will pre-populate 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 DAC. 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 through a common application.
- Department of Labor (DOL)
  - DOL shares information with DAIP pertaining to benefit programs available to the applicant based on questions answered by the user (no PII is shared).
- Food for Florida (FFF)
  - Under routine use H, DAIP shares disaster applicant information for applicants who live in the State of Florida and are seeking Disaster Supplemental Nutrition

Assistance Program (DSNAP) benefits, a Florida state benefit program. Applicant information is shared via secure web services to Florida's Department of Children and Families (DCF) FFF to pre-register the applicant for food assistance. Registration must be completed in person by the applicant at a designated center prior Florida making any financial eligibility or assignment determination.

- IdP
    - Under routine use F, DAIP has contracted with an IdP service and shares applicant information (title or prefix, name, SSN, and DOB are required; middle initial and email address are optional). DAIP shares this information because the IdP provides identity verification, identity authentication, and pre-population of tele-registrar screens at NPSC call centers.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Any sharing of DAIP/DAC information is compatible with the original purpose for collection in DHS/FEMA-008 Disaster Recovery Assistance Files System of Records, 74 FR 48763, September 24, 2009, and is only shared consistent with the published routine uses therein. The routine uses are also compatible with the original purpose of the collection to register, verify, and determine the eligibility of applicants needing disaster assistance; inspect damaged homes; and prevent duplication of federal government efforts and benefits.

6.3 Does the project place limitations on re-dissemination?

Yes. All sharing of DAIP/DAC information is compatible with the original purpose for collection, as noted in Section 6.2 above. In addition, DAIP does not share information without a demonstrated "need to know" the information requested. The information sharing agreements between DAIP and each participating agency covers technical and security requirements for the sharing and transmission of data and that the data not be re-disseminated.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

As identified in the DHS/FEMA-008 Disaster Recovery Assistance Files System of Records, 74 FR 48763, September 24, 2009, requests for records from DAIP/DAC are made to the FEMA Disclosure Office, which maintains the accounting of what records were disclosed and to whom. In addition, DAIP/DAC may electronically share records with partner agencies, and in such cases, details are logged about each transaction including the date and time of the transaction, and the specific data that was sent to each agency, and the status of the transaction.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a privacy risk that DAIP/DAC could erroneously disclose information

Mitigation: This privacy risk is mitigated because DAIP only shares the information in DAIP/DAC outside of DHS pursuant to the routine uses published in the DHS/FEMA-008 Disaster Recovery Assistance Files System of Records, 74 FR 48763, September 24, 2009, and only using appropriate security controls as outlined in the ISAs that have been are approved for each agency transaction. In addition, DAIP restricts the access of its partner agencies to only that information relevant to their respective programs, and only to those individuals with a "need to know" for the specific data.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

Disaster assistance applicants can access their information in several other ways: 1) applicants may access their information online via DAC using the user ID, password, system generated PIN, and authentication that was established during the application process; 2) applicants may call a NPSC representative to check on the status of their application by providing their registration ID; and 3) applicants receive a hard copy of their completed Form 009-0-1 as part of the mail-out package after registration.

DAIP processes disaster assistance requests from the registrations taken by the DAC system, which is part of the DHS/FEMA-008 Disaster Recovery Assistance Files System of Records, 74 FR 48763, September 24, 2009. Applicants for disaster assistance may consult the SORN for additional information regarding how to access their respective disaster application files via a Privacy Act or Freedom of Information Act (FOIA) request submitted to the FEMA Disclosure Office. Such requests should be sent to: FEMA Disclosure Officer, Records Management Division, 500 C Street, SW, Washington, DC 20472.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals may correct inaccurate information on-line by authenticating into the DAIP/DAC system and making whatever edits are required. If online access is unavailable, individuals should notify DAIP of the error/inaccuracy through one of the procedures noted in 7.1 above, and provide DAIP with the correct information. For inaccurate data that requires correction from an external agency, applicants can request that agency to correct his or her record in accordance with their applicable policies.

7.3 How does the project notify individuals about the procedures for correcting their information?

DHS/FEMA-008 Disaster Recovery Assistance Files System of Records, 74 FR 48763, September 24, 2009, and this PIA provide notice regarding how disaster survivors applying for assistance through DAIP/DAC can correct their disaster application information. In addition, after registration through the DAIP/DAC system, each applicant receives a mail-out package, which includes an application guide with directions for redress in a section entitled, "I Want to Have My Case Reviewed Again (Appeal)."

Disaster survivor applicants may also call FEMA's Help Line (1-800-621-FEMA) or log into their online account to review their current information on file and provide updates as appropriate.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a privacy risk that disaster survivors applying for assistance through DAIP/DAC will be unable to complete the online application because they do not pass the IdP verification process or the IdP authentication process and are unaware of the redress process.

Mitigation: DAIP mitigates this privacy risk by providing several means of redress to applicants who wish to amend their disaster assistance registration information. DAIP provides applicants with a direct notice of redress in the mail-out packages sent to each applicant, as noted in Section 7.1 above. DAIP also provides redress through its NPSC staff, whom applicants may contact toll-free via telephone (1-800-621-FEMA). In addition, DAIP uses a manual process for applicants who return a fail flag from the IdP, which mitigates the impact upon the applicant should DAIP receive erroneous information from the IdP. Lastly, the DHS/FEMA-008 Disaster Recovery Assistance Files System of Records, 74 FR 48763, September 24, 2009, and this PIA provide notice of redress processes to disaster assistance applicants.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

DAIP ensures that the practices stated in this PIA are followed by leveraging training, policies, rules of behavior, SOPs, information security agreements, auditing, and accountability.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All DAIP employees and contractors are required to successfully meet annual privacy awareness and information-security training requirements according to FEMA training guidelines. DAIP provides supplementary security-related training to those with additional security-related responsibilities. All contract employees are required to adhere to the Privacy Act and confidentiality clauses per terms of their contracts with DAIP.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

DAIP employees and authorized IT contractors will have restricted, role-based access to DAIP/DAC 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 ISAAC 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. Additionally, all internal end users are required to read and sign a rules of behavior agreement.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

DAIP/DAC coordinates the combined effort of federal, tribal, state, local, and non-profit agencies/organizations through a MOU with each participant that describes the working agreement between DAIP and the participant and the responsibilities of each. If data is to be transmitted between DAIP and another entity, an ISA is generated to govern the security of data and identify the necessary protective measures that must be maintained to safeguard privacy of personal information.

FEMA's process for reviewing and approving MOUs and ISAs involves FEMA's IT Security Branch, FEMA Privacy Officer, and the Office of Chief Counsel, in addition to the DAIP Program Manager, as well as the appropriate authorities from the other agency/organization to the agreement. FEMA will review these agreements on an annual basis and review appropriate security documents for any newly identified risks. FEMA will mitigate any newly identified risks between the partnering agencies in accordance with applicable laws.

Responsible Officials

Eric M. Leckey
Privacy Officer
Federal Emergency Management Agency
U.S. Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office.

____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security

Appendix A: FEMA Forms and OMB Control Numbers

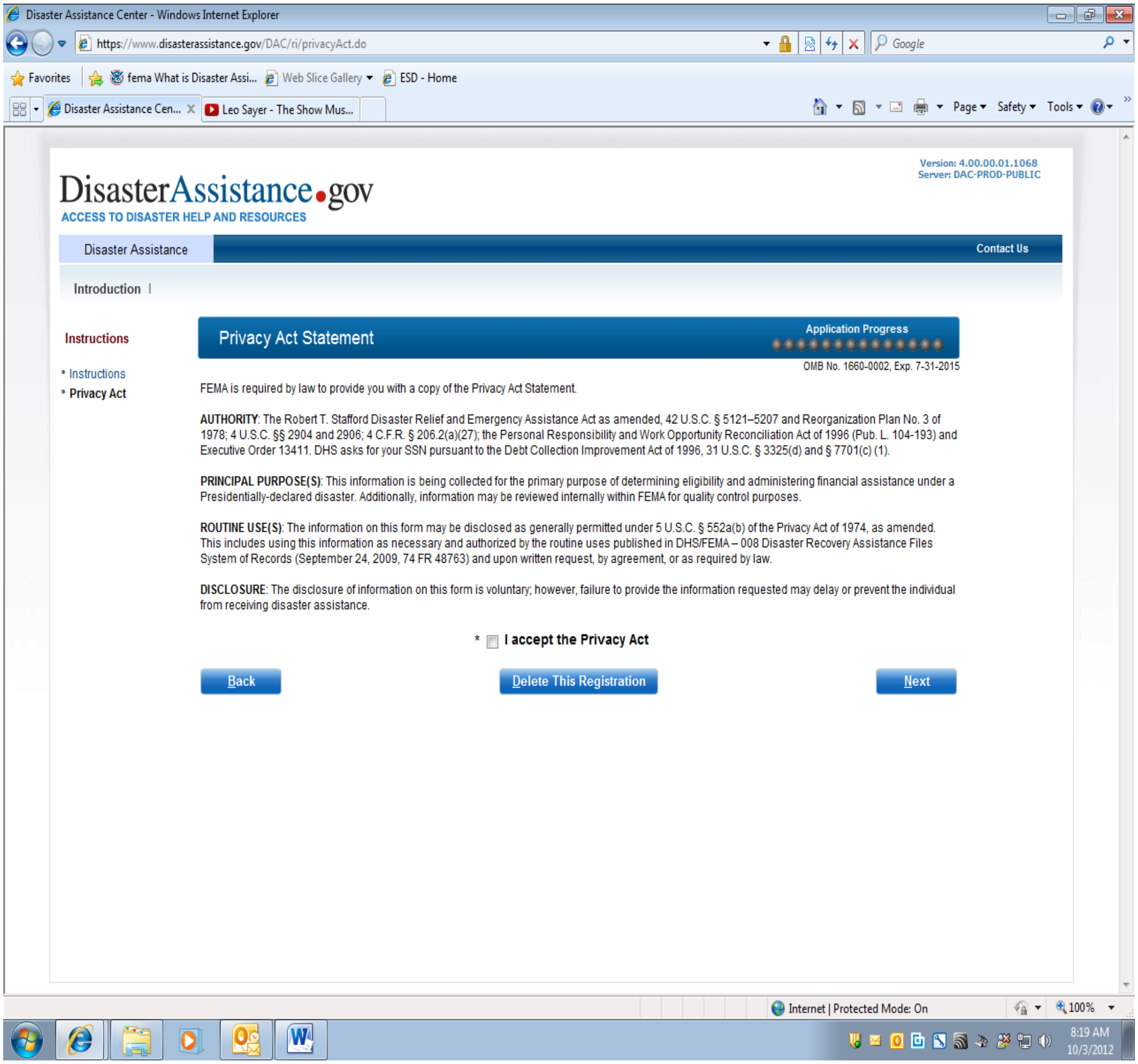
- OMB Control No. 1660-0002, “Disaster Assistance Registration:”
  - FEMA Form 009-0-1 (English), “Application/Registration for Disaster Assistance:”
  - FEMA Form 009-0-1T (English), “Tele-Registration, Application for Disaster Assistance:”
  - FEMA Form 009-0-1Int (English), “Internet Application/Registration for Disaster Assistance:”
  - FEMA Form 009-0-1S (English), Smartphone, Disaster Assistance Registration:”
  - FEMA Form 009-0-2 (Spanish), “Solicitud en Papel / Registro Para Asistencia De Desastre:”
  - FEMA Form 009-0-2Int (Spanish), “Internet, Registro Para Asistencia De Desastre:”
  - FEMA Form 009-0-2S (Spanish) “Smartphone, Registro Para Asistencia De Desastre:”
  - FEMA Form 009-0-3 (English), “Declaration and Release Form:”
  - FEMA Form 009-0-4 (Spanish), “Declaración Y Autorización:”
  - FEMA Form 009-0-5 (English), “Temporary Housing Program-Receipt for Government Property:” and
  - FEMA Form 009-0-6 (Spanish), “Recibo de la Propiedad del Gobierno.”
- OMB Control No. 1660-0061, “Federal Assistance to Individuals and Households Program:”:
  - FEMA Form 010-0-11, “Administrative Option Selection:” and
  - FEMA Form 010-0-12, “Application for Continued Temporary Housing Assistance.”

Appendix B – Acronyms List

DAC	Disaster Assistance Center
DAIP	Disaster Assistance Improvement Program
DCF	Department of Children and Families (Florida)
DHS	Department of Homeland Security
DOB	Date of Birth
DoED	Department of Education
DOL	Department of Labor
DRA SORN	Disaster Recovery Assistance System of Record Notice
DSNAP	Disaster Supplemental Nutrition Assistance Program
FEMA	Federal Emergency Management Agency
FFF	Food for Florida
FOIA	Freedom of Information Act
IA	Individual Assistance
IAC	Individual Assistance Center
ICD	Interface Control Document
IdP	Identity Proofing
IHP	Individuals and Households Program
ISA	Interconnection Security Agreement
ISAAC	Integrated Security and Access Control
IT	Information Technology
MOU	Memorandum of Understanding
NARA	National Archives and Records Administration
NEMIS	National Emergency Management Information System
NPSC	National Processing Service Center
NSLDS	National Student Loan Data System
OMB	Office of Management and Budget

PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIN	Personal Identification Number
PRA	Paperwork Reduction Act
SBA	Small Business Administration
SOA	Services Oriented Architecture
SSA	Social Security Administration
SSN	Social Security Number

Appendix C: DisasterAssistance.gov Privacy Act Statement


Disaster Assistance Center - Windows Internet Explorer
https://www.disasterassistance.gov/DAC/ri/privacyAct.do
Favorites
fema What is Disaster Assi...
Web Slice Gallery
ESD - Home
Disaster Assistance Cen...
Leo Sayer - The Show Mus...
Page
Safety
Tools
DisasterAssistance.gov
ACCESS TO DISASTER HELP AND RESOURCES
Version: 4.00.00.01.1068
Server: DAC-PROD-PUBLIC
Disaster Assistance
Contact Us
Introduction
Instructions
Instructions
Privacy Act
Application Progress
Internet | Protected Mode: On
100%
8:19 AM
10/3/2012

Privacy Act Statement

OMB No. 1660-0002, Exp. 7-31-2015

FEMA is required by law to provide you with a copy of the Privacy Act Statement.

AUTHORITY: The Robert T. Stafford Disaster Relief and Emergency Assistance Act as amended, 42 U.S.C. § 5121–5207 and Reorganization Plan No. 3 of 1978; 4 U.S.C. §§ 2904 and 2906; 4 C.F.R. § 206.2(a)(27); the Personal Responsibility and Work Opportunity Reconciliation Act of 1996 (Pub. L. 104-193) and Executive Order 13411. DHS asks for your SSN pursuant to the Debt Collection Improvement Act of 1996, 31 U.S.C. § 3325(d) and § 7701(c) (1).

PRINCIPAL PURPOSE(S): This information is being collected for the primary purpose of determining eligibility and administering financial assistance under a Presidentially-declared disaster. Additionally, information may be reviewed internally within FEMA for quality control purposes.

ROUTINE USE(S): The information on this form may be disclosed as generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act of 1974, as amended. This includes using this information as necessary and authorized by the routine uses published in DHS/FEMA – 008 Disaster Recovery Assistance Files System of Records (September 24, 2009, 74 FR 48763) and upon written request, by agreement, or as required by law.

DISCLOSURE: The disclosure of information on this form is voluntary; however, failure to provide the information requested may delay or prevent the individual from receiving disaster assistance.

* ☐ **I accept the Privacy Act**