Privacy Impact Assessment
for the

DisasterHelp.Gov (DHelp) Web Portal

December 19, 2006

Contact Point
Chip Hines, PMP
Program Manager
Disaster Management e-Gov Initiative
Command, Control & Interoperability
Science and Technology Directorate
Department of Homeland Security
(202)-254-6742

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(571) 227-3813

Abstract

The DisasterHelp.Gov (DHelp) website or web portal is operated by the Science and Technology Directorate of the Department of Homeland Security.[1] It is intended to assist political and civil service leadership, emergency managers, homeland security advisors, and first responders in the execution of their disaster management responsibilities. The information on this website will be used to enhance disaster management on an interagency and intergovernmental basis by helping users find information and services. The types of personally identifiable information used will include contact information for these individuals. The collection of this personally identifiable information is the reason for this privacy impact assessment.

Introduction

The DHelp web portal is one of several responses to Congressional concerns with the country's ability to respond to and mitigate disasters. Requirements for this web portal included the implementation of a nationally scalable interoperable data sharing environment for Citizens, Responders, Businesses, Government, and Non-government organizations. The DHelp web portal provides "one stop" shopping for references and collaboration tools pertaining to disaster preparation, mitigation, response and recovery.

DHelp has three levels of functionality and the amount and type of personal information collected is commensurate with the level of personalization: 1) public access to the web site, 2) registered user with personalized content, and 3) validated registered users with access to community of interest, collaboration areas, and a searchable list of validated users known as the "White Pages". The public facing portal can be readily accessed by individuals without the need for collecting any personal information. If an individual desires to utilize additional features of the portals such as personalization, custom content channels, or to subscribe to Disaster News Notification, they need to register as a public user and give a very minimal amount of personally identifying information.

Registering for DHelp allows individuals to customize their own personal page, which allows the placement of the information that they select in a single location. When individuals logs onto DHelp they will see all of the channels they have placed there, and thus be given quick and easy access to specific information. A major benefit of being a registered user is an individual's ability to create his own custom channels to pull together links or web pages.

In the near future, an individual can choose to become a validated registered user, whereby the individual's employer will validate the role. Being a validated registered user allows individuals to have access to additional functionality and information, including a directory of other validated users in a given community. These custom channels can also be placed on an individual's customized role page for easy access. The various available include: Citizen, Responder (Emergency Medical Technician (EMT), Fire, Police, Medical, and Emergency Manager), Military, Government Civilian Agency Employee, Other and, "I prefer not to respond").

[1] The Name of this System is: DisasterHelp.gov web portal (DHelp). The Unique System Number is: 024-00-01-08-01-0130-24-104-010 (Capital Planning UPI Code). The DHS Component who owns this system is: Command, Control & Interoperability, Science and Technology Directorate (S&T), Department of Homeland Security

For example, a registered user who is also validated as a First Responder will have access to additional features (beyond the access of a public user) including access to the DHelp Enterprise Collaboration Center (ECC) thus facilitating the sharing of emergency management information across the country. Validated First Responders will also have access to the DHelp ECC that serves as a knowledge sharing center allowing validated users to upload and download documents into the relevant community knowledge centers. The ECC is organized by community (e.g. Police, Hazmat, etc.), making it fast and easy to locate information. Registered public users can become registered validated users if they have a valid '.gov', '.mil', '.us' e-mail addresses, or they are authenticated responders. Additionally, registered validated users (i.e., individuals with '.gov', '.mil', '.us' e-mail addresses, and authenticated responders) get access to expanded features including: customized channels, a customized personal page, and, for validated users, access to the Enterprise Collaboration Center, plus DisasterHelp Instant Messenger and Chat. This exchange of information does not include personally identifiable information. A public registered user can apply to be a validated user by submitting a request with the additional information as described in paragraph 1.1 above.

The contact information collected and maintained by DHelp will be accessed principally by the responder community and other disaster management agencies at the Federal, state, local, foreign, or tribal level, who, in accordance with their responsibilities, are lawfully engaged in collecting emergency related information. Each of these parties will be granted on very limited access related to the specific disaster (e.g.. if Town X has a disaster, they can only access disaster information related to Town X.)

The DHelp portal provides a gateway to share disaster information and applications, links to other government Internet sites, ability to collaborate with other users to share ideas and resources, and allow an authorized, registered user to customize layout and presentation. DHelp allows access to disaster related information from one source, communications with the emergency management community, sharing of documents, view pertinent news and headlines, chat and meet online, start and follow threaded online discussions, as well as subscribe to emergency related notifications

The DHS Privacy Office has identified the need for a System of Records Notice (SORN) to cover certain functionality related to the DHelp portal. The DHS SORN 004 - General Information Technology Access Account Records System will cover the additional functionality for sharing contact information in the DHelp system. To ensure compliance with the Privacy Act the Disaster Management Program Office and the DHS OCIO have implemented a phased approach for system services and capabilities that will avoid activities that:

1. Share contact information to validate an individual is associated with a given organization, and

2. Share information in the White Pages.

These services and capabilities will not be enabled until the Systems of Records Notice (SORN) identified as DHS/ALL 004, General Information Technology Access Account Records System, has been issued. In the interim, the SORN DHS/ALL 002, Mailing Lists and Contacts, 69 FR 233, December 6, 2004, covers the more limited collection and use of information.

Section 1.0
Information collected and maintained

The following questions are intended to define the scope of the information requested as well as the reasons for its collection as part of the system, rule, and/or technology being developed.

1.1 What information is to be collected?

Phase I collection

General Public
When a member of the general public (as a public user) visits the DHelp web portal, the following information about a visit is automatically collected and stored, as long as the system is in operation:

- The Internet domain and the IP address from which the website is accessed;
- The type of browser and operating system used to access the site;
- The date and time the site is accessed;
- The pages visited; and
- If linked to disasterhelp.gov from another website, the address of that website.

Registered Users
A minimum set of voluntary information is submitted by an individual when they choose to become a registered user. That information is:

- Last Name;
- First Name;
- E-mail address;
- Expertise or Role in disaster management;
- Zip code;
- Yes/no answer for a subscription to *Disaster News*.

Upon Phase II collection when new SORN is published and operational.

Validated Registered Users
Validated registered users have access to knowledge centers where they can read, download, and upload documents/files. The following additional information that may be collected from a registered user who wishes to become a validated user are:

- Business organization;
- Position within the business organization;
- POC Name (used to verify the registrant);
- POC e-mail address;
- POC telephone number.

With Phase II, contact information of validated registered users will be available to all validated registered users in the same community of interest. A registrant is required only to make available to other validated users a minimum of personally identifiable information in order to become enrolled in the portal's list of validated users known as the White Pages. Specifically, only the first and last name, e-mail, and zip code of

the individual are required for the White Pages; other information such as phone and address can be removed from the profile by the user and will not be displayed in the White Pages. The "White Pages" feature will not be available until the overarching DHS/ALL 004, General Information Technology Access Account Records System System of Records Notice has been issued and is operational. The additional POC information needed to become validated registered users is maintained in the system database and is only accessible to portal administrators responsible for validating registered users.

1.2 From whom is information collected?

For DHelp, personally identifiable information is collected directly from those individuals requesting access to the additional features of the DHelp web portal as registered users or validated registered users. These individuals come from a various range of roles including: Private Citizen, Responder (EMT, Fire, Police, Medical, and Emergency Manager), Military, and Government Civilian Agency Employees. The information collected may vary by role according to how much access to the site the person desires (see Introduction and question 1.1).

When a user registers as a validated registered user he must provide the name of his sponsoring organization, the name of a point of contact (POC) in the sponsoring organization and the associated phone number and/or e-mail address of the POC. To ensure compliance with the Privacy Act the Disaster Management Program Office and the DHS OCIO have implemented a phased approach for system services and capabilities that will avoid activities that involve employer or group association contact or that share contact information to validate an individual. These activities will not be undertaken until the Systems of Records Notice identified as DHS/ALL- 004 has been issued.

1.3 Why is the information being collected?

DHS intends to use the information collected and maintained by DHelp to identify individuals who have registered with the site to gain access to additional disaster management resources, such as the Collaboration Center, while at the same time facilitating access to resources for the general public.

1.4 How is the information collected?

Most PII collected is typed by the individual user into the web portal via the browser using a web form. PII collected from employers or sponsoring organizations is used for validation of end user accounts. The requesting user enters the sponsoring organization and POC in the DHelp online registration form. This information is validated by the DHelp Administrator who telephones and/or e-mails the POC to verify the legitimacy of the user's request. The DHelp Administrator also verifies the legitimacy of the sponsoring organization as a member of the First Response Community.

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

The DHelp web portal was developed in accordance to the E-Government Act of 2002, specifically Section 214, *Enhancing Crisis Management through Advanced Information Technology*.

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

Privacy risks identified include the individual not being aware that his personal information will be available on the White Pages and the threat of identity theft and malicious modifications of the information posted in the White Pages. In order to mitigate the lack of awareness, DHS has issued a new SORN – DHS/ALL 004 that provides notice of this sharing. Notice will also be provided at the time of collection on the web site for validated registered users. The White Pages feature will not be available until the DHS SORN-004 is published in the Federal Register.

In order to mitigate the threat of identity theft and malicious modification of the information posted in the White Pages, the following mitigation strategies have been taken:

- Not allowing the White Pages data to be downloaded or transmitted to external systems; and
- Restricting the viewing of the White Pages only to validated registered users. This viewing capability will only return 200 records in any one search, and will only display ten records at a time.

DHelp collects and stores this voluntary information that is provided from the individual**.** Any information obtained from a registered or validated registered user is voluntary and the individual has the option to select "I prefer not to respond" when asked about his or her role. This functionality allows an individual to tailor to personal preferences the information he or she is releasing to the DHelp.

Section 2.0
Uses of the system and the information

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

2.1 Describe all the uses of information.

DHS intends to use the information collected and maintained by DHelp to carry out its disaster management, disaster response, and other functions including:

- Increase overall preparedness, particularly for catastrophic events; and
- Enhance information sharing within the disaster management community.

The collection of the POC information in the context of the ECC communities (see Introduction) provides those communities with an instant network of colleagues and peer-professionals. This allows for greater communication among similarly situated professional involved in disaster and/or emergency management. This information will not be used in this manner until the SORN DHS/ALL 004 has been published and is operational.

Non-identifying site management information is collected for statistical purposes. Software routinely collects information to create summary statistics that assess what information is of most and least interest to the visitors to the web site; to determine technical design specifications; to identify system performance or problem areas; to summarize the number of visitors to the web site; and to survey the types of technology that the visitors use.

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

No. The data collected is not assimilated, altered, manipulated, or aggregated in a way that would lead to new data or a view of the data that was previously unavailable. There are no processes or code within the system that permit creation of new data through aggregation or derivation. The White Pages are searchable but are not analyzed in any way.

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

During the validated registered user validation process DHS may contact the sponsoring organization's point of contact (POC) submitted by the applying user. To ensure compliance with the Privacy Act the Disaster Management Program Office and the DHS OCIO have implemented a phased approach for system services and capabilities that will avoid activities that involve employer or group association contact or share contact information to validate an individual is associated with a given organization. These activities will not be undertaken until DHS/ALL-004 System of Records Notice has been published.

2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.

Taken in context with the limited scope of the collection of contact information, the uses of the information are limited to communication and collaboration efforts amongst emergency management personnel and first responders. No other information is required for the proper functioning of DHelp. Therefore, the uses described in Section Two are commensurate with the reasons for the collection of the information outlined in Section One. The controls described in Section Eight outline the protections provided the amount or scope of information collected in DHelp.

Section 3.0 Retention

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

3.1 What is the retention period for the data in the system?

For DHelp, the only information normally retained on individuals is how to contact them and the information necessary to validate their access to the applications. This contact information is generally

professional contact information. Registration data is incorporated into end-user account data and is retained as long as the user account remains active.

Aggregated meta-data for site access and use data is retained in accordance with NARA General Records Schedule 24 "Information Technology Operations and Management Records", until 3 years old, for site development and maintenance purposes. This deletion is done by the database administrator manually.

For information uploaded into the collaboration center DHS will expunge this information after one year in the absence of consent from the owner. The administrator for Knowledge Center is notified when documents have reached the expired date and can renew the data or let it permanently expire after 30 days at which time it gets deleted.

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

The contact information for creating the user accounts are retained and disposed of in accordance with the National Archives and Records Administration's General Records Schedule 24, section 6, "User Identification, Profiles, Authorizations, and Password Files,". Inactive records will be destroyed or deleted 6 years after the user account is terminated or password is altered, or when no longer needed for investigative or security purposes, whichever is later.

For additional information created by the collaboration center, the program is working with the DHS records officer to determine an appropriate timeframe.

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

The contact information is maintained for a limited period of time after the account is inactive based on NARA schedule. Other information posted in the collaboration center will be scheduled with NARA in the future.

Section 4.0
Internal sharing and disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organizations is the information shared?

DHS system administrators may have access to the data for maintenance of the system and to ensure that the system's applications work correctly. This access is part of the normal day-to-day operation of the infrastructure for the system.

The White Pages contact information is available to all registered users within the restricted collaboration ECC in the DHelp Portal. Once within a community all users may see the White Pages information of their fellow community members whether they are employees or contractors for DHS, private citizens, responders from any organization or whether they are federal, state or local, Fire, Police, Medical, and Emergency Professionals, or Military. Please note that the White Pages feature will not be available until the DHS/ALL-004 SORN has been published and is operational.

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

The efficient sharing of information can only be accomplished by creating a Knowledge Center where individuals accepted as members of a collaboration center are granted specific levels of access for specifically targeted information. Personal contact information may be provided by the originator (information manager) via the White Pages within the restricted collaboration section of DHelp for use by other emergency response organizations, such as those at the international, federal, state, and local levels. The data is to be used for coordinating emergency responses. The White Pages feature will not be available until the DHS/ALL-004 SORN has been published.

4.3 How is the information transmitted or disclosed?

Data exchange, between a user and the DHelp web portal, takes place over an encrypted transmission session.

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

To counter the risk that the PII may be released without proper authorization, DHS system administrators and users of the web portal must sign and acknowledge a set of rules of behavior governing their activities, and acknowledging that they have been trained and understand the security aspects of this information system. These individuals are also required to undergo periodic security awareness training that includes protection for privacy data under their control.

Section 5.0
External sharing and disclosure.

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes Federal, state and local government, and the private sector.

5.1 With which external organizations is the information shared?

The user organizations, utilizing DHelp, include the 32 partner agencies making up the Office of Management & Budget's (OMB's) e-Gov initiative. Although DHelp is available to the general public, these

organizations form an integrated team of partner agencies and organizations that perform Disaster Management activities. The Disaster Management e-Government Initiative is focused on providing information and services relating to the four pillars of all-hazards disaster management: preparedness, response, recovery, and mitigation. Additional services will incorporate delivery of integrated, cross-agency processes and services to citizens, governments, and NGOs with emphasis on First Responder needs. The partner agencies include:

- The American Red Cross;
- The Appalachian Regulatory Commission;
- The Coordinated Assistance Network;
- The Department of Agriculture;
- The Commerce Department;
- The Department of Education;
- The Department of Defense;
- The Department of Energy;
- The Department of the Interior;
- The Department of Justice;
- The Department of Labor;
- The State Department;
- The Department of Transportation;
- The Nuclear Regulatory Commission;
- The Emergency Information Infrastructure Project;
- The Environmental Protection Agency;
- The Federal Communication Commission;
- The Federal Communication Commission;
- The General Services Agency;
- Health and Human Resources;
- Housing and Urban Development;
- The Internal Revenue Service;
- The National Aeronautics and Space Administration;
- The National Oceanographic and Atmospheric Agency;
- The National Traffic Safety Board;
- The Office of Personal Management;
- The Small Business Administration;
- The Social Security Administration;
- The Tennessee Valley Authority;
- The United States Agency for International Development;
- The Unites States Postal Service;
- The veterans Administration;
- State and local governments; and
- Other non-governmental organizations.

The White Pages contact information is available to all validated registered users within the restricted collaboration ECC in the DHelp Portal. Once within a community all users may see the White Pages information of their fellow community members whether they are employees or contractors for DHS, private citizens, responders from any organization or whether they are federal, state or local, Fire,

Police, Medical, and Emergency Professionals, or Military. Please note that the White Pages feature will not be available until the DHS/ALL-004 SORN has been published.

5.2 What information is shared and for what purpose?

Information placed on the public portion of the DHelp web portal by DHS is unclassified, non-sensitive information authorized for public release to provide disaster management information. This information will **not** include personally identifiable information.

The contact information collected and maintained by DHelp will be accessed by the responder community and other disaster management agencies at the federal, state, local, foreign, or tribal level that are validated registered users. This information, organization, company phone, etc.., is provided by the DHelp users in accordance with his responsibilities. DHelp validated registered users exchange information through DisasterHelp.gov as coordinating parties to support all phases of Disaster Management including preparedness, response, and recovery. Each of these parties will be granted very limited access related to the specific disaster. (e.g. If Town X has a disaster, they can only access disaster information related to Town X.)

The DHelp portal provides a gateway to share disaster information and applications, links to other government Internet sites, ability to collaborate with other users to share ideas and resources, and allow an authorized, registered user to customize layout and presentation. DHelp allows access to disaster related information from one source, communications with the emergency management community, sharing of documents, view pertinent news and headlines, chat and meet online, start and follow threaded online discussions, as well as subscribe to emergency related notifications.

5.3 How is the information transmitted or disclosed?

Data exchange, between a user and the DHelp web portal, takes place over an encrypted transmission session through the Internet.

Information posted on the web portal is downloaded using the user's web browser.

Individuals do not need to register to use the public portions of the DisasterHelp.gov portal. Without registering, they will have access to the large amount of information available on public community pages that do not include personally identifiable information. This session is encrypted to protect the confidentiality of the transmission.

5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

There is no Memorandum of Understanding in place with any external organization for the sharing of personally identifiable information. Validated registered users having access to DHelp which includes the White Pages must agree to the terms of use "warning banner" every time they logon. The terms of use

addresses appropriate/required conduct. If they do not click "Ok" to agree to terms of use they are unable to logon and thus will denied access to the White Pages. The White Pages feature will not be available until the DHS/ALL-004 SORN has been published.

5.5 How is the shared information secured by the recipient?

DHS does not maintain control of any information a public user, registered user, or validated registered user may download or print from the DisasterHelp.gov web portal, including information from the White Pages. The White Pages are not allowed to be downloaded or transmitted to external systems. Please note that the White Pages feature will not be available until the DHS/ALL-004 SORN has been published.

The information collected and maintained by DHelp is designed to be shared with the emergency responder community, and to a lesser degree, with the public. In general the disaster management e-government initiative is focused on providing information and services relating to the four pillars of all hazards disaster management: Preparedness, Response, Recovery, and Mitigation. The information provided to the public includes openly available disaster management information and resources provided by the 32 partner agencies as described in Section 5.1 of this PIA. Additional services will be provided to the emergency responder community through roll based access controls defined and administered inside the DHelp system. Examples of these services include secure exchange of documents through collaboration centers, and the ability to assess, track, and report their organization's readiness status.

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

There is no formal training required for users of outside agencies prior to gaining access to DHelp. DHS users and administrators receive security and privacy training in accordance with their employment obligations. The Privacy and Security Link includes the Privacy Act Notification statement, which includes sharing of the personal information in the White Pages. The White Pages feature will not be available until the DHS/ALL-004 SORN has been published.

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

Privacy risks identified include the individual not being aware that his personal information will be available on the White Pages and the threat of identity theft and malicious modifications of the information posted in the White Pages. In order to mitigate the lack of awareness, DHS has issued a new SORN – DHS/ALL 004 that provides notice of this sharing. Notice will also be provided at the time of collection on the web site for validated registered users. The White Pages feature will not be available until the DHS SORN-004 is published in the Federal Register.

In order to mitigate the threat of identity theft and malicious modification of the information posted in the White Pages, the following mitigation strategies have been taken:

- Not allowing the White Page data to be downloaded or transmitted to external systems; and
- Restricting the viewing of the White Pages only to registered or verified registered users. This viewing capability will only return 200 records in any one search, and will only display ten records at a time.

The White Page information is not broadcast or distributed in any way other than through the Portal to registered users within a community. The White Pages feature will not be available until the DHS/ALL-004 SORN has been published

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

Yes, a posted privacy policy is available for viewing on the web site. A copy of this notice is provided in Appendix A of this document. The DHS Privacy Office has identified the need for a System of Records Notice. (SORN) to cover DisasterHelp.gov. The DHS Privacy Office is currently working with Counsel on a broad DHS SORN that would cover this type of activity. Until DHS/ALL-004 SORN is published DHelp will not enable the following services and capabilities;

1. Share contact information to validate an individual is associated with a given organization, and
2. Share information in the White Pages.

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

Yes. Individuals are informed that they are not required to give their personally identifying information if they want to use the public sections of the DHelp website. However, if they opt to use the private sections of DHelp they are voluntarily opting in by providing their personally identifying information.

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

right?

The Privacy Act Notification Statement posted on the DisasterHelp.gov web site (Appendix A) informs the user of the uses of the information he/she may provide while visiting or entering information on this portal. The user may either consent to the stated uses of their personal identifying information or choose not to participate in the web portal as a registered user.

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

The risk of insufficient notice as it relates to sharing of information was identified and is being mitigated through the publishing of a new SORN that will cover the functionality of the validated user and the White Pages. Until this SORN is published and operational, these functionalities will not be available. Additional notice of the sharing is included in the Privacy Act Notification statement provided at the time of collection so that individuals will be made aware of the sharing.

Section 7.0
Individual Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures which allow individuals to gain access to their own information?

A registered user of the DisasterHelp.gov web portal can view their profile information, which is maintained on them in the DHelp portal. No individual user can view the profile data of another registered user.

An individual with questions or concerns regarding any personally identifiable information that may be maintained in this information system may request those records from:

U.S. Department of Homeland Security
Under Secretary for Science & Technology
Cynthia Christian, FOIA Officer
Washington, D.C. 20528

7.2 What are the procedures for correcting erroneous information?

Registered users may correct any entry they made of by accessing their profile through the DHelp portal application. The Dhelp application is also supported by a service desk that can provide additional assistance where needed through an on-line hyperlink from the web page, www.disasterhelp.gov/portal/jhtml/customization/feedback.jhtml or by calling 1-800-451-2647.

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

Individuals are notified of the procedures for correcting as stated above in section 7.2.

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

Redress is provided, so alternatives are not applicable.

7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, explain the procedural rights that are provided and, if access, correction and redress rights are not provided please explain why not.

The access and procedural rights for Privacy Act data is stipulated in paragraph 7.1 above. Also, technical tools are provided to allow users to change their contact information. Because of the ample measures in place, the risks associated with inaccurate information and user access are minimal.

Disclaimers are in place on the web pages as to the validity of the information placed by individuals or organizations other than the Federal government, and also to any information found by following the in-place hypertext links or through searchers for information posted on the World Wide Web.

Section 8.0
Technical Access and Security

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

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

Access to the publicly available information (that does not include personally identifiable information) will be granted to private citizens who have been authenticated by appropriate emergency management points of contact at Federal, state and local levels of government. Key examples would be local firefighters or emergency medical technicians requiring collaborative capabilities for exchanging information unique to an incident – past or present. Access within DHelp to a collaboration center (work) or application is granted only by the administrator for the collaboration center. The administrator is designated by the emergency management community owner responsible for operating the collaboration center. In most cases the emergency management community owner is not a DHS employee nor contractor. In the DHelp distributed environment it is the responsibility of the collaboration center owner to establish a vetting process for granting access and rules of use/behavior.

Full access to all personally identifiable information is granted only to a few individuals based upon their official roles as managers overseeing the program and system administrators who maintain the system. As an E-Government initiative, senior managers require complete access to manage the delivery of Disaster Management functionality. System Administrators, Data Base Administrators, developers, and testers may have access to the data for maintenance of the system and to ensure the application works correctly. This access is part of the normal day-to-day operation of the infrastructure for the system.

The contact information collected and maintained by DHelp will be accessed principally by the responder community when that phase of functionality begins. Additionally, the information may be shared with other disaster management agencies at the federal, state, local, foreign, or tribal level, who, in accordance with their responsibilities, are lawfully engaged in collecting emergency related information. DHelp does not share contact data with other systems nor do other systems have access to contact data within DHelp. Personal contact information may be provided by the originator (information manager) via the White Pages list of registered users within the restricted collaboration section of DHelp for use by other emergency response organizations, such as those at the international, federal, state, and local levels. The data is to be used for coordinating emergency responses.

8.2 Will contractors to DHS have access to the system?

Yes, contractors will have limited/full access to the system for the limited purposes of the maintenance and operation of the system, which includes ensuring data integrity, correct application functionality and availability, and data confidentiality.

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

Yes, access to the DHelp web portal is role based. Disaster Management roles are:

Public Users	Browse public content View USDA disaster designations View the latest disaster-related news and headlines
Registered Users	Create a personal page to display information they are interested in all in one place. Sign up for USDA disaster notifications at the county and state level.
Validated Registered Users	Sign up for EMR-ISAC Critical Infrastructure Protection notifications Participate in discussion forums Exchange documents securely in the collaboration center Assess, track and report on readiness status
Public Content Administrators	Edit public pages under their control and create new pages for their community

Systems Operation Roles

Data Center Manager	Has physical access to production servers, databases and network infrastructure (e.g., firewalls, routers); has functional access to production servers.
Database Administrator	Has physical access to production databases and infrastructure (e.g., firewalls, routers); has system administration rights to production databases; has functional access to production servers.
IT Security Officer/Manager	Has supervised physical access to production servers, databases and infrastructure (e.g., firewalls, routers); has functional access to production servers on an as needed basis; may conduct penetration testing and/or ST&E testing on production servers.
Network Administrator	Has physical access to production servers, databases and infrastructure (e.g., firewalls, routers); has system administration rights to production servers; has functional access to production servers.
Program Manager	Has functional access to production servers.
Programmer/Systems Analyst	Has functional access to production servers.
System Administrator:	Has physical access to production servers, databases and infrastructure (e.g., firewalls, routers); has system administration rights to production servers; has functional access to production servers.
System Designer/Developer	Has functional access to production servers.
Systems Operations Personnel	Has physical access to production servers, databases and infrastructure (e.g., firewalls, routers); has system administration rights to production servers; has functional access to production servers
Technical Support Personnel	Has supervised physical access to production servers, databases and infrastructure (e.g., firewalls, routers); has supervised system administration rights to production servers on an as needed basis; has functional access to production servers on an as needed basis.

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

When an individual requests to join a new community,, the community administrator reviews and approves or denies their request through the DHelp collaboration center software. Users can request access to any public collaboration center, but must be invited to any private collaboration center by the center administrator.

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

Access to the restricted modules or collaboration center is requested by an authorized DHS employee or contractor who manages the module or collaboration center. DHelp provides audit trail information, which contains the below information extracted from audit trail documentation. Module or collaboration center site administrators can use these audit trails to verify system usage. The auditing requirements are included below:

- "Update" includes insertions of new data, deletion of existing data, and edits of existing data.
- The time of any update must be recorded.
- The user logged into the system, the "actor," must be recorded.
- The object acted upon must be recorded. This object could be a group, a page, a channel, a user, or any other piece of content in Appian Enterprise. There is no requirement to record the nature of the change made to the object. That is, while we must know that a link was added to a links channel, we do not need to know what the URL and text of that link are. Likewise, when a link is deleted, we do not need to know which one.
- The audit trail must be stored in a format that is readable by DHS security personnel. Such formats may include flat files or databases.
- The audit trail must indicate which application is the source of the audit (e.g. DHelp core or a side application).

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

DHS employees and/or contractors that are involved in auditing and technical maintenance of are designated by the role they perform and their access to the DHelp application is audited in compliance with DHS MD 4300A. Audit Trail logging has been enabled on DHelp as described in section 8.5.. The site administrators for the restricted modules are provided with read access to a web page containing the results of this auditing for the module under their jurisdiction. These audit records show the noted actions of the individual's access to the module, the pages visited, and a date/time stamp of the activity.

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

DHS employees are required to undergo annual security and privacy training. Aside from the privacy notification posted on the DHelp web portal, there is no privacy training provided to the non-DHS users of the DHelp web portal.

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

The data is secured in accordance with FISMA requirements. The Disaster Management Systems program will secure information on the DHelp web portal by complying with the requirements as stated the DHS IT Security Program Handbook (DHS 4300A). This handbook establishes a comprehensive program, consistent with Federal law and policy, to provide complete information security, including

directives on roles and responsibilities, management policies, operational policies, and application rules, which will be applied to component systems, communications between component systems, and at interfaces between component systems and external systems. The DHS MD 4300A security requirements were incorporated into requirements for the development of the DHelp application,

The DHelp web portal received a 3 year Authority to Operate (ATO) on June 17, 2004. DHelp has recently completed the re-certification process for accreditation to operate, with renewed 3 year ATO granted on December 5, 2006 .

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

Since DHelp contains both a public and a private portal, an identified threat exists that non-public information may leak or be accessed by the public. To counter this threat:

- Passwords for the registered users are secured in an encrypted database table. Additionally, standard password access controls are placed on user accounts; and
- The entire session is encrypted to protect the integrity and confidentiality of the transactions over the Internet.

DHelp applies the Departmental standard in system security. Strong and clearly defined user controls and auditing help protect not only the personally identifiable information contained on DHelp but also help maintain system integrity as a whole.

Section 9.0 Technology

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

9.1 Was the system built from the ground up or purchased and installed?

This system was built from the ground up and is a key element of the Disaster Management E-Gov Initiative and provides direct support for meeting Presidential Management Agenda requirements as identified in the "Quicksilver" task fore report of FY 2002.

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

Data integrity, privacy and security were considered early on in the analysis and incorporated into the formally established system requirements. These requirements were traced through the development and verified/validated in the system test phase.

9.3 What design choices were made to enhance privacy?

At the web portal, Secure Socket Layer (SSL) FIPS 140-2 validated encryption is used to protect the integrity and confidentiality of the transaction. Application access is provided by a centralized, load balanced firewall service that acts as an integration point for all Internet, intranet, and extranet network connections. Role/group based security is incorporated into DisasterHelp.gov. This enables users to post different levels of information. The program also created different level of access so that certain functionality that includes the sharing of personal information is only done when individuals have been validated as being in the proper community of interest.

Conclusion

Legislation both before and after the events of September 11, 2001 led to the development of the web portal DisasterHelp.gov under the Disaster Management e-Government Program. The program is based on Congressional concerns with the country's ability to respond to and mitigate disasters. Requirements for the program included the implementation of a nationally scalable interoperable data sharing environment for Responders.

Based on this analysis, it can be concluded that

- The DHelp web portal creates a pool of individuals whose professional information, and potentially some voluntarily provided personal information is at risk;
- The administrators of the DHelp web portal have mitigated the specific privacy risks caused by non-DHS employees using the White Pages by requiring individuals to be validated before using the White Pages functions, by providing notice of how the White Pages works, and by providing notice of the appropriate use of the White Pages functions.
- Secure Socket Layer (SSL) encryption is used to protect the integrity and confidentiality of the transaction.

RESPONSIBLE OFFICIALS

Chip Hines
Program Manager
Disaster Management e-Gov Initiative
500 C St SW
Washington, DC 20472
202-646-3115
Chip.hines@dhs.gov

Chandler Sirmons
Director, Enterprise Applications Delivery and Operations (EADO)
System Owner for Enterprise Portals (including Diasterhelp.gov)
Office of the Chief Information Officer (OCIO)
Infrastructure Operations (IO)
7th & D Streets, S.W.
Washington, DC 20024
202-447-0285
chandler.sirmons@dhs.gov

Approval Signature

_____

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security

Appendix A
Privacy Act Notifications

The following is the Privacy and Security Notice from the DisasterHelp.gov web site:

Viewer Privacy and Security Notice

Introduction

1. Disasterhelp.gov is one of 24 eGovernment initiatives sponsored by the Office of Management and Budget (OMB) focused on improving services to the citizen. The Department of Homeland Security Science and Technology Directorate (DHS S&T) has been designated the managing agency partner for this initiative.

2. This World Wide Web (WWW) site is provided as a public service by the Department of Homeland Security Science and Technology Directorate (DHS S&T) and its initiative partners.

3. Information presented on this WWW site is considered public information and may be distributed or copied. Use of appropriate byline/photo/image credits is requested.

4. This WWW site references and links to a large number of public and private sites. We have provided a link to these sites because they have information that may be of interest to our viewers. DHS does not necessarily endorse the views expressed or the facts presented on these sites. DHS does not endorse any commercial products that may be advertised or on these sites. The DHS Privacy Notice Policy does not apply on these sites. Please check the site for its Privacy Notice.

Information collected and stored automatically

1. The information we learn about you from your visit to our website depends upon what functions you perform when visiting our site.

2. For site management, information is collected for statistical purposes. This government computer system uses software programs to create summary statistics, which are used for such purposes as assessing what information is of most and least interest, determining technical design specifications, and identifying system performance or problem areas.

3. If you do nothing during your visit but browse through the website, read pages, or download information, we will gather and store certain information about your visit automatically. This information does not identify you personally. We automatically collect and store the following information about your visit:

-The Internet domain (for example, "xcompany.com" if you use a private Internet access account, or "yourschool.edu" if you connect from a university's domain) and IP address (an IP address is a number that is automatically assigned to your computer whenever you are surfing the web) from which you access our website;

- The type of browser and operating system used to access our site;

- The date and time you access our site;

- The pages you visit; and

- If you linked to disasterhelp.gov from another website, the address of that website.

We use this information to help us make our site more useful to visitors -- to learn about the number of visitors to our site and the types of technology our visitors use. We do not track or record information about individuals and their visits.

Cookies
The only cookies DHS uses on its web are those that allow several complex software user-driven applications to work correctly. For instance, our online ordering services (for publications of the U.S. Fire Administration and for the FEMA Flood Map Store) allow users to "shop" through the catalog. As a user goes through and checks off a series of publications, each transaction is a separate "signal" sent between their computer and ours. In order to maintain a complete record of the total order, the ordering server sends a cookie to identify that user's order. The only information collected is related to that particular publication order and this information is NOT retained once the order is sent.

This is the state of technology on the web. There currently exist no non-cookie applications for this multi-order function.

Please be assured that DHS's use of cookie technology is NOT a covert attempt to either collect or analyze information on Internet users.

Information Collected from E-mails and Web Forms

If you identify yourself by sending an E-mail or using web Forms:

You also may decide to send us personally-identifying information, for example, in an electronic mail message containing a complaint or compliment. We use personally-identifying information from viewers in various ways to further the usefulness and accuracy of the information contained on our web site or to add new sections and services. Visit Feedback, on the homepage of https://disasterhelp.gov to learn what can happen to the information you provide us when you send us e-mail.

We want to be very clear: We will not obtain personally-identifying information about you when you visit our site, unless you choose to provide such information to us.

Information collected on a voluntary basis for validating registered users

For DHelp, personal identifying information is collected from those individuals requesting access to the additional features of the DHelp web portal as registered users or validated registered users. These individuals come from a various range of roles including: Private Citizen, Responder (EMT, Fire, Police, Medical, and Emergency Manager), Military, and Government Civilian Agency Employees. The information collected may vary by role according to how much access to the site the person desires (see Introduction and question 1.1). When a user registers as a “validated user” they must provide the name of their sponsoring organization, the name of a point of contact (POC) in their sponsoring organization and the associated phone number and/or e-mail address of the POC. Personally Identifiable Information (PII) is provide on a voluntary basis, there are only 5 mandatory fields (username, first name, last name, e-mail, and zip code), users can edit their profile to remove information provided (with exception of the

mandatory fields), and only registered/validated users through authenticated login can view the White Pages. Please note that the White Pages feature will not be available until the overarching DHS SORN has been completed. Collected information from employers regarding verification of status is maintained inside the user's request record and is accessible by the DHelp Administrators and Database Administrators.

Additionally, to ensure compliance with the Privacy Act the Disaster Management Program Office and the DHS OCIO have implemented a phased approach for system services and capabilities that will avoid activities that involve employer or group association contact or share contact information to validate an individual is associated with a given organization. These services and capabilities will not be enabled until the Systems of Records Notice (SORN) identified as DHS 002, General Information Technology Access Account Records System, DHS/ALL 004. System of Records Notice has been issued. In the interim, the SORN DHS/All 002, Mailing Lists and Contacts covers the more limited collection and use of information.

Security and Intrusion Detection

1. For site security purposes and to ensure that this service remains available to all users, this government computer system employs software programs to monitor host and network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.

2. Except for authorized law enforcement investigations, no other attempts are made to identify individual users or their usage habits. Raw data logs are used for no other purposes and are scheduled for regular destruction in accordance with National Archives and Records Administration guidelines.

3. Unauthorized attempts to upload information or change information on this service are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act."