Privacy Impact Assessment
for the

Web Portal for the Center for Faith-based and Community Initiatives

January 10, 2007

Contact Point
Keith Rothfus
Center for Faith-based and Community Initiatives
Preparedness Directorate
202-786-9552

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

Abstract

This project will create a web-based portal to enable individuals to register their names and email addresses in order to receive information about the activities of the Center for Faith-based and Community Initiatives (CFBCI) at Department of Homeland Security (DHS). The collection of contact information will enable the CFBCI to disseminate information to interested parties. Because the contact information qualifies as personally identifiable information under the E-Government Act of 2002, this privacy impact assessment has been conducted.

Introduction

This project will create a web-based portal which will enable individuals to register their names and email addresses in order to receive information about the activities of the Center for Faith-based and Community Initiatives at DHS. Presidential Executive Order 13397 directs DHS to "develop and coordinate Departmental outreach efforts to disseminate information more effectively to faith-based and other community organizations with respect to programming changes, contracting opportunities, and other agency initiatives, including but not limited to Web and Internet resources." DHS is implementing a "comprehensive outreach and technical assistance strategy" that employs ten best practices for faith-based outreach. Two of those best practices relate to the creation of a database of faith-based and community organizations and individuals interested in DHS programs. This web portal will ensure that DHS is compliant with its obligations under Executive Order 13397.

Potential users will access the CFBCI website through www.DHS.gov. From the CFBCI link on DHS.gov visitors may submit contact information through pre-set contact information fields. This contact information populates a simple database which is accessed by CFBCI employees in order distribute updates, bulletins, and announcements from the CFBCI.

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?

The portal will collect name, business address, business phone, and email address from interested parties.

1.2 From whom is information collected?

This information is collected directly from individuals interested in receiving updates on the efforts of the CFBCI.

1.3 Why is the information being collected?

The information is collected in order for the CFBCI and DHS to easily disseminate information to parties interested in the CFBCI's outreach efforts in accordance with Presidential Executive Order 13397.

1.4 How is the information collected?

Information is collected through the web portal where interested parties can voluntarily submit their contact information. The transfer of information is in electronic digital form.

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

Presidential Executive Order 13397 directs DHS to "develop and coordinate Departmental outreach efforts to disseminate information more effectively to faith-based and other community organizations with respect to programming changes, contracting opportunities, and other agency initiatives, including but not limited to Web and Internet resources."

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.

To mitigate risk, CFBCI collected the minimum amount necessary directly from the individual in order to distribute the information requested by the individual, whether by mail, electronic mail, or by phone.

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.

The information is used to contact individuals through outreach efforts of the CFBCI.

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

No.

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

The CFBCI information will not check information for accuracy. CFBCI presumes that an individual who desires to receive information from the CFBCI will give the correct information. If information is found to be invalid in some way it will be deleted by CFBCI employees.

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.

CFBCI will use the data collected only for the express purposes of notifying interested parties of upcoming events of interest, including conferences of interest to faith-based and community organizations and DHS grant and policy announcements. CFBCI will not transfer the data to third parties and CFBCI employees accessing the data will be advised that the database content is not to be forwarded to third parties unless cleared through the Privacy Office and Office of the General Counsel.

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?

DHS Senior Records Officer's preliminary assessment indicates General Records Schedule (GRS)14, Item 1 for "information request files" will apply. Files will be deleted when three (3) months old, or no longer needed for administrative purposes, or last use of the information for contact purposes.

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

The Center for Faith-based and Community Initiatives is currently working with the DHS Senior Records Officer to develop a final disposition schedule which will be sent to NARA for approval.

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

CFBCI has consulted with the DHS Records Officer and received a proposed schedule, but until the schedule is finalized and approved by NARA all data will be considered permanent. The preliminary determination for the retention schedule maintains the information for a period relevant to its use.

Section 4.0 Internal Sharing and Disclosure

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

4.1 With which internal organizations is the information shared?

The information will be used only within the CFBCI.

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

The information is not shared.

4.3 How is the information transmitted or disclosed?

The information is not shared.

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

No risks were identified in this PIA.

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 information will not be shared externally.

5.2 What information is shared and for what purpose?

The information will not be shared externally.

5.3 How is the information transmitted or disclosed?

The information will not be shared externally.

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?

The information will not be shared externally.

5.5 How is the shared information secured by the recipient?

The information will not be shared externally.

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

The information will not be shared externally.

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

The information is not shared with any external groups. No risks were identified.

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?

A Privacy Act statement will be posted on the website prior to collection explaining CFBCI and DHS will not use the information for any other purpose than to send out relevant information on CFBCI efforts. The statement is attached at Appendix A. This system is covered by System of Records Notice DHS/All-002, DHS Mailing and Other Lists Systems (69 FR 70460).

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

Yes.

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?

No. If the individual is submitting his information it is for the sole purpose of receiving information from the CFBCI on CFBCI initiatives.

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

Notice is given to potential enrollees in the mailing lists through this PIA, the System of Records Notice, and notice through the website that the collection of personal information is voluntary and information is used for a limited purpose. Specifically, (e)(3) notice under the Privacy Act is given to any person prior to the relinquishment of personal information.

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?

Individuals will be able to request information they previously submitted by contacting the CBFCI. The CBFCI's email address will be provided on the CFBCI web site. This will allow individuals to update submitted information at any time.

7.2 What are the procedures for correcting erroneous information?

CFBCI staff will review emails from individuals inquiring about their data and will make appropriate revisions if so requested.

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

Individuals are notified on the sign up page of the procedures to correct information.

7.4 If no redress is provided, are alternatives available?

Redress is provided.

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.

Redress measures are provided to individuals. Allowing individuals to freely update information through the CFBCI email address and contact information reduces the risk of inaccurate information by directly involving those who submit information.

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?

The data submitted will be added to a database that will be accessible by CFBCI staff only.

8.2 Will contractors to DHS have access to the system?

At this time the CFBCI does not employ contractors.

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

The information collected from the web site will be auto-populated into either a Microsoft Access Database or Excel Spreadsheet. These files will be stored on a DHS network server and password protected and accessible only to CFBCI staff who have individual log-in IDs and passwords.

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

The data will be in password-protected files accessible only by CFBCI staff. CFBCI employees accessing the database will have already cleared DHS Security for background check.

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

The data will be in password-protected files accessible only by CFBCI staff. Should new staff join the CFBCI they will be briefed on the proper use of the contact information.

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

The data will be in password-protected files accessible only by CFBCI staff. Given the simplicity of the system, no auditing or specific technical measures are in place other than the access controls described in 8.1 through 8.5 as well as those associated with DHS.gov as a whole.

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

CFBCI employees are advised that the data contained in the database is to be used for the limited purpose of informing interested parties of information relevant to CFBCI efforts or DHS programs and policies, and that the data is not to be shared with third parties.

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

DHS.gov, upon which the CFBCI site rests, received its Authority to Operate from the Chief Information Security Officer on September 20, 2006. Certification and Accreditation has been completed and will be renewed in 2009 per the mandatory three (3) year renewal process.

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

Privacy risks include outside hackers accessing the system and CFBCI with access to the database making an unauthorized disclosure. CFBCI staff will be advised that the data in the database is not to be transferred to third parties absent Privacy Office and OGC approval. Additionally, CFBCI staff receive annual security and privacy training required by DHS. CFBCI will rely on Departmental firewalls and security mechanisms to protect the database from outside hackers.

The system has received an ATO and meets DHS standards.

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?

DHS Infrastructure personnel along with CFBCI personnel will be building the web interface within DHS.gov.

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

CFBCI understands the risks associated with the collection of personally identifiable information. This PIA has been conducted in part to assess those risks and identify mitigation steps where necessary.

9.3 What design choices were made to enhance privacy?

The data will be housed on a DHS server in a password protected file accessible only to authorized CFBCI personnel.

Conclusion

The data collected through the web interface will be stored on a DHS server in a password protected file. CFBCI will operate on DHS servers which have passed C & A inspection and are employing reasonable measures to prevent unauthorized access to such servers.

Responsible Officials

Keith Rothfus
Center for Faith-based and Community Initiatives
Preparedness Directorate
202-786-9552

Approval Signature Page

_____ January 10, 2007

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security

Appendix A

This Privacy Act statement is presented to any person prior to the collection of personal information.

Privacy Act Notice

Authority: Presidential Order 13397 authorizes the collection of information in order to disseminate information concerning DHS's faith-based and community organization outreach.

Purpose: DHS's Center for Faith-based and Community Initiatives (CFBCI) is collecting this information in order to disseminate information more effectively to faith-based and other community organizations with respect to programming changes, contracting opportunities, and other agency initiatives.

Routine Uses: The contact information will not routinely be disclosed outside of the CFBCI, or outside of DHS; However, information in limited instances may also be disclosed pursuant to the published system of records notice (DHS/All-002 (69 FR 70460)).

Disclosure: Providing information to the CFBCI is voluntary. Refusal to provide contact information will result only in not receiving outreach from the CFBCI.