Privacy Impact Assessment
for the

Department of Homeland Security
General Contact Lists

June 15, 2007

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

Abstract

Many Department of Homeland Security operations and projects collect a minimal amount of contact information in order to distribute information and perform various other administrative tasks. Department Headquarters has conducted this privacy impact assessment because contact lists contain personally identifiable information.

Overview

The Department's mission encompasses a wide variety of activities, including: emergency response, law enforcement and intelligence, critical infrastructure protection, immigration processing, and research and development of new technologies. In order to facilitate the accomplishment of these activities the Department is in constant contact with the public as well as partners in other federal, state, local, and international governmental organizations (hereinafter known as "partners"). Part of the Department's interaction with the public and its partners involves the maintenance of very limited contact information. For example, a member of the public may request mail or email updates regarding emergency response procedures, or partners working on cross-agency project may need to be able to contact their peers. These types of situations require the exchange of minimal contact information in order to facilitate the Department's operations and service to the public.

Accordingly, DHS collects limited contact information such as name, email address, and mailing address. Many times names and phone numbers are not required for mass distribution lists. Other times name and business affiliation, in addition to basic contact information, will be collected in order to facilitate a working relationship between partners.

General information intake involves the following:

An individual person will contact the Department via phone, paper form, or electronically (web or email) for the purpose of being added to an information distribution list. In order to accommodate that request, the person will provide basic contact information (depending on the circumstances) such as his or her name, mailing address, email address, and phone number. DHS then places the contact information in a spreadsheet, database or other type of information management tool. The Department then accesses the information from its storage site and uses it to distribute information or contact users per the confines of their interaction with DHS.

The authority to collect the information lies within each program or project's authorizing legislation.

Any program or project seeking to use this PIA as privacy documentation for its contact list must meet the following requirements:

1. The contact information is limited to non-sensitive personally identifiable information. An example of sensitive personally identifiable information is the social security number or date of birth.
2. The program or project must affirm that the document or database in which the contact information is stored resides on a system that has received an Authority to Operate from the Chief Information Security Officer.

3. The program or project must affirm that user access controls are in place governing who may view or access the contact information. The contact information must not be universally accessible.
4. The contact information must only be used for the purpose for which it originally was collected, i.e., to contact individuals. Any additional sharing or use will require a separate PIA.

Should a program or project feel its contact list meets these requirements, the program or project is required to complete a Privacy Threshold Analysis (PTA) detailing how it has met these requirements. Once the PTA is approved, the program or project's name and component will be added to Appendix B of this document as a qualifying program or project.

Section 1.0 Characterization of the Information

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

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

Contact lists generally include name, business affiliation, mailing address, phone number, and email address. Sensitive personally identifying information such as a social security number or date of birth are not covered under this PIA. Such collections are required to conduct separate PIAs analyzing the risks associated with such sensitive collections.

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

Information is collected directly from individuals seeking information from the Department, or who are working collaboratively with the Department on various projects. Individuals provide their information voluntarily.

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

The information is collected to facilitate the dissemination of information regarding the Department's operations and to facilitate the collaboration of partners who are working with the Department on various projects.

1.4 How is the information collected?

Information may be collected electronically, by paper form, or by telephone.

1.5 How will the information be checked for accuracy?

Information is collected directly from individuals who volunteer information and is assumed to be accurate. Depending on the context of the collection, the project or program may conduct a certain degree of verification of information and follow up with an individual if information is found to be inaccurate.

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

Programs are at a minimum authorized to collect and maintain contact information by the Homeland Security Act of 2002. Specific legal authorities for this type of collection are established based on each component and each program's particular mission. Nonetheless, some programs may operate under specific rules, regulations, treaties, or other statutes pertinent to their field.

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

The privacy risk presented by a basic contact list is that more information will be collected than is necessary to distribute information. Contact information is limited to the information necessary to perform the information distribution functions of the program or project. All information is collected with the consent of the individual.

Section 2.0 Uses of the Information

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

2.1 Describe all the uses of information.

The Department uses the information to contact individuals.

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

Information is stored but is not manipulated in any way other than to, if necessary, populate address fields for a mass email or paper mailing. Data may be input into databases or electronic spreadsheets and accessed via the various data elements. For example, a query may be conducted to locate all contacts in a certain state.

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

Contact lists are not created, populated with, or verified with data collected from commercial or publicly available sources.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

The risk presented by the use of contact information is that the information would be used in ways outside the scope intended by the initial collection. Per the System of Records Notice DHS/All 002 (69 FR 70460, December 6, 2004) and the Privacy Act Statements given prior to collection, information collected for contact lists is not to be used for any other purpose than to contact individuals who have requested particular information. Additionally, all Department employees and contractors are trained on the appropriate use of personally identifiable information.

Section 3.0 Retention

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

3.1 How long is information retained?

The Department retains the information no longer than is useful for carrying out the information dissemination or collaboration purposes for which it was originally collected. Individuals may request their information be deleted if he or she is no longer interested in receiving information from the Department, after which point their information will not be retained. Absent a more restrictive retention period for a particular contact list, information is retained per the requirements of General Records Schedule 14, Informational Services Records (see Question 3.2).

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

Records are retained and disposed of in accordance with the National Archives and Records Administration's General Records Schedule 14. Files may be retained for up to six years. For requests that result in litigation, the files related to that litigation will be retained for three years after final court adjudication.

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

Information is retained for no more than six years after the last use. This minimizes retention and security costs associated with maintaining contact lists. Additionally, any individual may opt out of any distribution list at any time in order to have their information expunged from the list, thereby eliminating any privacy risks posed by retention of their contact information.

Section 4.0 Internal Sharing and Disclosure

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

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

Contact information may be shared with internal DHS components inasmuch as they are involved in distributing information or collaborating with partners within the Department. However, DHS does not share contact information for any purpose beyond which it was originally collected, i.e. contact information given by individuals for purpose *x* will not be shared for use of purpose *y* at a later date.

4.2 How is the information transmitted or disclosed?

DHS may share information by electronic or paper means. If information is transmitted electronically, proper security measures are taken, including encryption when necessary.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Inappropriate sharing is a risk inherent to any collection of personally identifiable information. Department employees and contractors are trained on the appropriate use and sharing of personally identifiable information. Further, any sharing of information must align with the purpose of the initial collection as well as the System of Records Notice DHS/All 002 (69 FR 70460, December 6, 2004) and the Privacy Act Statement provided at the time of collection.

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

Contact information may be shared with external governmental entities inasmuch as those entities are involved in distributing information or collaborating with partners within the Department. Nonetheless, contact information is not shared for any purpose beyond which it was originally collected, i.e. contact information given by individuals for purpose *x* will not be shared for use of purpose *y* at a later date.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

Yes. Per the System of Records Notice DHS/All 002 (69 FR 70460, December 6, 2004) and the various notices provided when information is collected, uses of contact information beyond the purposes for which it was originally collected is not acceptable.

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

Any information shared with organizations outside the Department is required to be appropriately secured per Office of Management and Budget Memorandums 06-15, Safeguarding Personally Identifiable Information, and 06-16, Protection of Sensitive Agency Information.

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

A risk is presented whenever the Department shares information it has initially collected from agencies or individuals outside of the Department. If external sharing of information would exceed the narrow purpose for which the contact information was collected, then the information is not permitted to be shared. The System of Records Notice DHS/All 002 (69 FR 70460, December 6, 2004) outlines the specific instances where contact information may be shared outside the Department. All Department employees and contractors are trained on the appropriate use and sharing of information.

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?

Yes. This privacy impact assessment and the System of Records Notice DHS/All 002 (69 FR 70460, December 6, 2004) provide notice regarding the collection of contact information by the Department. More appropriately, though, each collection of contact information is immediately preceded by notice regarding the scope and purpose of the contact information at the time of collection. These Privacy Act Statements (these notices are required under 5 U.S.C. § 552a(e)(3)) at the moment of collection provide individuals with notice of the voluntary nature of the collection and the authority to collect the information.

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

Yes. Individuals are not required to provide contact information. Nevertheless, if contact information is not provided individuals may not receive information from the Department or from partners in the Department.

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

DHS will use the information only for the purposes for which it was collected, i.e., contacting individuals. Should an individual suspect information is being used beyond the given scope of the collection, they are encouraged to write to the system managers listed in Appendix A. The system managers are also listed in the System of Records Notice DHS/All 002 (69 FR 70460, December 6, 2004).

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

The privacy risk associated with notice in the collection of contact information is that the individual is not aware of the purpose for which the information he or she submits may be used. This risk is primarily mitigated by limiting the use of contact information to what is necessary for the purposes of contacting the person according to his or her voluntary subscription or request. Additionally, the System of Records Notice DHS/All 002 (69 FR 70460, December 6, 2004) provides notice of the purpose of the collection, redress procedures and the routine uses associated with the collection of contact information. Notice is always provided prior to the collection of information, and consent is obtained by the individual prior to his providing information.

Section 7.0 Access, Redress and Correction

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

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

Should individuals seek to remove their name from a contact list they should write or call the program or project which initially collected the information. The program or project is in the best position to remove, edit and/or provide access to the information held on an individual. Access requests can also be directed to FOIA / PA D-3, The Privacy Office U.S. Department of Homeland Security, 245 Murray Drive SW, Building 410, STOP-0550, Washington, DC 20528-0550.

Additionally, the System of Records Notice DHS/All 002 (69 FR 70460, December 6, 2004) details access provisions along with the names of officials designated to field such requests within the Department.

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

The procedures are the same as those outlined in Question 7.1. The program or project that initially collected the information is in the best position to correct any inaccurate information. Any inquires for correction should be made to the initial collector.

Additionally, the System of Records Notice DHS/All 002 (69 FR 70460, December 6, 2004) details access provisions along with the names of officials designated to field such requests within the Department.

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

Individuals are notified at collection that they may correct their information at any time by the procedures outlined above.

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

Appropriate redress is provided.

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

Individuals may correct their information at any time during which the Department possesses and use their contact information. Any risks associated with correction of information are thoroughly mitigated by the individual's ability to opt out of the contact list or correct their information via the same process by which they submitted information.

Section 8.0 Technical Access and Security

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

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

Departmental physical and information security policies dictate who may access Department computers and filing systems. Specifically, DHS Management Directive 4300A outlines information technology procedures for granting access to Department computers, which is where the majority of contact information is stored. Access to contact information is strictly limited by access controls to those who require it for completion of their official duties.

8.2 Will Department contractors have access to the system?

Yes, depending on the project or program. Many times contractors are tasked with information distribution and other outreach tasks. Contractors are required to have the same level of security clearance in order to access Department computers as all other DHS employees.

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

All Department employees and contractors are required to receive annual privacy and security training to ensure their understanding of proper handling and securing of personally identifiable information such as what is contained in contact lists.

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

Most simple contact lists are stored on spreadsheets or similar formats that do not qualify as an information technology system requiring a Certification and Accreditation (C&A) pursuant to the review processes established by the Chief Information Security Officer; however, these documents are stored on secure Department networks which have completed C&As. Other contact lists which are part of more robust functionalities reside on information technology systems that are required to receive a C&A.

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

All Department information systems are audited regularly to ensure appropriate use and access to information. Specifically related to contact information, such lists residing on a local area network's shared drive are restricted by access controls to those who require it for completion of their official duties. Folders within shared drives are privilege-protected.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

The risk of unauthorized access exists with any information technology system or document. The Department conducts thorough background checks on every employee and contractor. Access to the systems and networks which store the contact information are protected pursuant to established Departmental procedures (see 8.4).

All Department employees and contractors are trained on security procedures, specifically as they relate to personally identifiable information.

Section 9.0 Technology

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

9.1 What type of project is the program or system?

This assessment covers contact lists developed by a program or project involved in outreach efforts or collaboration efforts within or outside of the Department.

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

The program or projects detailed here are not necessarily involved in a specific lifecycle. Complete information technology systems are in the operational phase and have completed C&A documentation. Individual contact information lists do not have a development cycle.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

If a particular technology used in the collection or handling of information in connection with the types of contact lists addressed in this PIA raises specific and/or heightened privacy concerns, the implementation of the technology will be required to conduct a separate PIA.

Approval Signature Page

Original signed and on file with the DHS Privacy Office

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security

Appendix A

I. For Headquarters components of the Department of Homeland Security, the System Manager is the Director of Departmental Disclosure, U.S. Department of Homeland Security, Washington, DC 20528.

II. For operational components that comprise the U.S. Department of Homeland Security, the System Managers are as follows:

United States Coast Guard, FOIA Officer/PA System Manager, Commandant, CG-611, U.S. Coast Guard, 2100 2nd Street, SW., Washington, DC 20593-0001

United States Secret Service, FOIA Officer/PA System Manager Suite 3000, 950 H Street, NW., Washington, DC 20223

United States Citizenship and Immigration Services, ATTN: Records Services Branch (FOIA/PA), 111 Massachusetts Avenue, NW, 2nd Floor, Washington, DC 20529

National Protection and Programs Directorate, FOIA Office, 3801 Nebraska Ave., NW, Nebraska Avenue Complex, Washington DC 20528

United States Customs and Border Protection, FOIA Officer/PA System Manager, Disclosure Law Branch, Office of Regulations & Rulings, Ronald Reagan Building, 1300 Pennsylvania Avenue, NW (Mint Annex)., Washington, DC 20229

United States Immigration and Customs Enforcement, FOIA Officer/PA System Manager, Office of Investigation, Chester Arthur Building (CAB), 425 I Street, NW., Room 4038, Washington, DC 20538

Transportation Security Administration, FOIA Officer/PA System Manager, Office of Security, West Building, 4th Floor, Room 432-N, TSA-20, 601 South 12th Street, Arlington, VA 22202-4220

Federal Protective Service, FOIA Officer/PA System Manager, 1800 F Street, NW., Suite 2341, Washington, DC 20405

Federal Law Enforcement Training Center, Disclosure Officer, 1131 Chapel Crossing Road, Building 94, Glynco, GA 31524

Under Secretary for Science & Technology, FOIA Officer/PA System Manager, Washington, DC 20528

Office of Intelligence and Analysis, 3801 Nebraska Ave., NW, Nebraska Avenue Complex, Washington DC 20528

Under Secretary for Management, FOIA Officer/PA System Manager, 7th and D Streets, SW., Room 4082, Washington, DC 20472

Office of Inspector General, Records Management Officer, Washington, DC 20528

Appendix B

Qualifying Programs or Projects

United States Citizenship and Immigration Services Customer Service Portal

Science and Technology Treaty Compliance Database

US Coast Guard Navigation Systems Information Dissemination Network

Infrastructure GovDelivery content subscription service

Infrastructure DHS Interactive

Customs and Border Protection Decal and Transponder Online Procurement System

National Protection and Programs Directorate Mission Operating Environment

Transportation Security Administration Contact Center System

Science and Technology Technical Evaluation System for Safety Act

National Protection and Programs Directorate Share Resources High Frequency Program

National Protection and Programs Directorate Master Station Log

Operations Directorate Personnel/COOP Database

Science and Technology HSARPA Broad Agency Announcement and Small Business Innovative Research

Science and Technology National Bio and Agro-Defense Facility (NBAF) Web page

Science and Technology BioWatch Web-Portal

National Protection and Programs Directorate Infrastructure Information Collection Program

Science and Technology Biodefense Knowledge Center (BKC) Subject Matter Expert (SME) Directory

Science and Technology Cyber Security Research and Development Center Web Site

US Coast Guard Proceedings magazine online subscription request form

Federal Emergency Management Agency National Fire Academy Long-Term Evaluation