Privacy Impact Assessment Update
for the

DHS General Contact Information

DHS/ALL/PIA-006(a)

April 25, 2019

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

Abstract

The Department of Homeland Security (DHS) has a responsibility to maintain accountability of its workforce and protect its personnel from harm. In order to accomplish those missions, DHS may collect emergency contact or next of kin information from personnel for the purpose of contacting those individuals in case of emergency. DHS is updating this Privacy Impact Assessment (PIA) to discuss the privacy risks of collecting personally identifiable information (PII) of members of the public who are listed as emergency contacts by DHS Headquarters and Component personnel.

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 working to achieve the Department's mission, there may be instances such as an emergency, incident, or other event that requires someone to reach out to an employee's designated emergency contact or next of kin. Accordingly, DHS may collect limited information about emergency contacts or next of kin. This information may include the following:

- Name;
- Work contact information (e.g., address, email address, phone number);
- Personal contact information (e.g., address, email address, phone number); and
- Relationship to DHS personnel or individual associated with the Department.

General information intake involves the following:

DHS requests information on individuals identified by current or former DHS personnel as emergency points of contact, including family members and next of kin. In certain circumstances, DHS may also request emergency contact information at training exercises or for disaster response activities.[1] Individuals supply this information to the Department and it is maintained 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 those individuals in the event of an emergency

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

[1] Pursuant to 42 U.S.C. § 5197(c), DHS, through FEMA, may also use Federal Government employees from other federal agencies who are deployed as a part of a mission assignment and non-Federal Government employees, such as other state, local, tribal, and territorial personnel.

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

- The contact information is limited to non-sensitive contact information, such as name, email address, and phone number.
- 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 (ATO) from the DHS Chief Information Security Officer. If records are maintained on paper, they should be stored in a locked drawer or file cabinet.
- The program or project must affirm that user access controls, or other methods, are in place governing who may view or access the contact information. The contact information must not be universally accessible.
- The contact information must only be used for the purpose for which it originally was collected (i.e., to contact individuals in the event of an emergency).

Reason for the PIA Update

DHS is updating this PIA to discuss the collection of emergency contact or next of kin information of DHS personnel or those associated with the Department. This information is needed for the purpose of contacting those individuals in case of emergency. The type of information is similar to the original DHS/ALL/PIA-006 DHS General Contacts List PIA. However, this PIA covers collecting this information from a new group of individuals for the specific reason for contacting an emergency contact in the event of an emergency.

Privacy Impact Analysis

Characterization of the Information

The information collected through this PIA Update is not substantially changing. Contact information generally consists of name, work contact information, personal contact information, and relationship to the DHS employee or individual associated with the Department who supplied the information.

However, information is not collected directly from the individuals to whom the information pertains. The information is collected from DHS personnel or individuals associated with the Department who have designated that individual as an emergency point of contact.

Although the information is not collected directly from individuals to whom it pertains, the information is collected from someone with a close relationship with that individual, and therefore it 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.

The information is strictly used for communication purposes in the case of emergency or the need to contact an emergency point of contact or next of kin.

The purpose and authorities for the collection and maintenance of this PII are outlined in the DHS/ALL-014 Department of Homeland Security Personnel Contact Information System of Records Notice (SORN).[2]

Privacy Risk: There is a risk that more information will be collected than is necessary.

Mitigation: This risk is mitigated. The contact information that is being collected is limited to what is necessary to contact the individual in the event of an emergency, incident, or other event that requires accountability. A program or project must follow the guidelines and requirements set forth in this PIA. Programs that require additional information or have different uses for the information may require a new PIA.

Uses of the System and the Information

The Department will continue to use the information collected to contact individuals only when there is an emergency or incident requiring the Department to reach out to an emergency contact. In the event of a personal incident or emergency, the administrator of the program or project maintaining the information, in consultation with management or the supervisor, may reach an individual's emergency contact in order to provide assistance to the individual.

Privacy Risk: There continues to be a risk that this contact information will be used in ways outside the scope intended by the initial collection.

Mitigation: The risk is mitigated through several factors. DHS stores this information on accredited systems that have sufficient security and privacy protections in place. DHS does not make this information universally available to everyone; user access controls or other methods are in place governing who may view or access the contact information. All Department personnel are trained on the appropriate use of PII.

Retention

The Department retains the information no longer than is useful for carrying out the communication purposes for which it was originally collected.

Individual designated to maintain the emergency contact list must review records relating to individuals designated as emergency points of contact and next of kin on an annual basis. The list will be updated as necessary, and will be destroyed when obsolete, or upon separation or transfer of the employee, in accordance with National Archives and Records Administration

[2] DHS/ALL-014 Department of Homeland Security Personnel Contact Information, 83 FR 11780 (March 16, 2018).

(NARA) General Records Schedule (GRS) GRS 5.3, Item 020 (DAA-GRS-2016-0004-0002).[3] Records on non-DHS individuals will be deleted when obsolete and of no longer use to the Department.

Privacy Risk: There is a risk that this information may be retained for longer than it is needed.

Mitigation: This risk is not fully mitigated. The retention period is outlined in this PIA and through NARA GRS 5.3, Item 020. However, this retention period is not clearly defined and it is incumbent on the program or project to ensure that the required measures are put in place to mitigate this risk.

Internal Sharing and Disclosure

Contact information may be shared internally throughout DHS based on a need-to-know and as necessary to provide assistance in the event of an emergency or incident. However, DHS does not share contact information for any purpose beyond that for which it was originally collected.

External Sharing and Disclosure

Contact information may be shared with external DHS partners as permitted by the DHS/ALL-014 DHS Personnel Contact Information SORN. However, DHS will not share contact information for any purpose beyond that for which it was originally collected.

Per the DHS Personnel Contact Information SORN, this information may be shared outside the Department to other governmental agencies or executive offices, relief agencies, and non-governmental organizations, when disclosure is appropriate for performance of the official duties required in response to emergencies or disasters (Routine Use I). For example, this information may need to be shared with a local emergency management agency who can better contact the next of kin of an employee during a local natural disaster.

Inappropriate sharing is a risk inherent to any collection of PII. Department personnel are trained on the appropriate use and sharing of PII and any sharing of information must align with the purpose of the initial collection as well as the DHS Personnel Contact Information SORN.

Notice

This PIA Update and the DHS Personnel Contact Information SORN provide notice regarding the collection of emergency contact or next of kin information by the Department. However, information is not collected directly from the individuals to whom the information pertains. The information is collected from DHS personnel or individuals associated with the Department who have designated that individual as an emergency point of contact or next of kin.

[3] *See* https://www.archives.gov/files/records-mgmt/grs/grs05-3.pdf.

Therefore, individuals may have no direct notice that their information is collected and maintained by DHS.

Individuals that have their information submitted as an emergency contact may not be able to opt out or consent to DHS's use of information. However, DHS will use the information only for the purposes for which it was collected (i.e., contacting individuals in case of an emergency).

Privacy Risk: There is a risk that individuals will not know that their information is being submitted to DHS.

Mitigation: This risk cannot be fully mitigated. Although this PIA Update and the DHS Personnel Contact Information SORN provide some notice regarding the collection of emergency contact or next of kin information by the Department, no direct notice is given to individuals. It is incumbent on the DHS personnel or individuals associated with the Department who submit the emergency contact or next of kin information to inform the individual that the personal information was given to the Department.

Individual Access, Redress, and Correction

Due to the nature of the collection of emergency contact or next of kin information, individuals may not know that the Department maintains information about them.

Individuals seeking access to and notification of any record contained within the DHS Personnel Contact Information system of records, or seeking to contest its content, may submit a request in writing to the Chief Privacy Officer and Headquarters or component's Freedom of Information Act Officer (FOIA), whose contact information can be found at https://www.dhs.gov/foia-contact-information.

If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to:

Chief Privacy Officer and Chief Freedom of Information Act Officer

Privacy Office, Department of Homeland Security

245 Murray Drive, SW, Building 410, STOP-0655

Washington, D.C. 20528

When an individual is seeking records about himself or herself from the DHS Personnel Contact Information system of records, the individual's request must conform to the Privacy Act regulations set forth in 6 CFR 5.

Technical Access and Security

Departmental physical and information security policies dictate who may access Department computers and information technology systems. Specifically, DHS Management Directive 4300A[4] outlines information technology procedures for granting access to Department computers, which is where the majority of emergency contact and next of kin information is maintained. Access to contact information is strictly limited by access controls to those who require it for completion of their official duties.

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.

Technology

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 or heightened privacy concerns, the implementation of the technology will be required to conduct a separate PIA.

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

_____

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

[4] *See* https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.