Privacy Impact Assessment
for the

<<ADD SYSTEM NAME>>

<<ADD Publication Date>>

Contact Point
<<ADD Type Contact Person>>
<<ADD Program/Agency/Office>>
<<ADD Component/Directorate>>
<<ADD Contact Phone>>

Reviewing Official
Maureen Cooney
Acting Chief Privacy Officer
Department of Homeland Security
(571) 227-3813

Abstract

The abstract should be a short paragraph, four sentences or less, that describe:

- The general type of information used.
- What the information is used to accomplish.
- Why it is important to use the information for that accomplishment.

<< ADD Abstract Here >>

Introduction

The introduction should contain the following elements, and should not exceed one page:

- The system name, the unique system number if there is one, and the name of the DHS component(s) that own(s) the system;
- The objective of the new program, technology and/or system and how it relates to the component's and DHS's mission;
- A general description of the information in the system and the functions the system performs that are important to the component's and DHS's mission; and
- A general description of the modules and subsystems, where relevant, and their functions. For longer more in depth descriptions, an appendix may also be appropriate.

<< ADD Introduction Here >>

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?

<< ADD Answer Here >>

1.2 From whom is information collected?

<< ADD Answer Here >>

1.3 Why is the information being collected?

<< ADD Answer Here >>

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

<< ADD Answer Here >>

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

<< ADD Answer Here >>

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.

<< ADD Answer Here >>

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”)?

<< ADD Answer Here >>

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

<< ADD Answer Here >>

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.

<< ADD Answer Here >>

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?

<< ADD Answer Here >>

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

<< ADD Answer Here >>

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

<< ADD Answer Here >>

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?

<< ADD Answer Here >>

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

<< ADD Answer Here >>

4.3 How is the information transmitted or disclosed?

<< ADD Answer Here >>

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

<< ADD Answer Here >>

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?

<< ADD Answer Here >>

5.2 What information is shared and for what purpose?

<< ADD Answer Here >>

5.3 How is the information transmitted or disclosed?

<< ADD Answer Here >>

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?

<< ADD Answer Here >>

5.5 How is the shared information secured by the recipient?

<< ADD Answer Here >>

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

<< ADD Answer Here >>

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

<< ADD Answer Here >>

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?

<< ADD Answer Here >>

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

<< ADD Answer Here >>

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?

<< ADD Answer Here >>

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

<< ADD Answer Here >>

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?

<< ADD Answer Here >>

7.2 What are the procedures for correcting erroneous information?

<< ADD Answer Here >>

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

<< ADD Answer Here >>

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

<< ADD Answer Here >>

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.

<< ADD Answer Here >>

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?

<< ADD Answer Here >>

8.2 Will contractors to DHS have access to the system? If so, please submit a copy of the contract describing their role to the Privacy Office with this PIA.

<< ADD Answer Here >>

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

<< ADD Answer Here >>

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

<< ADD Answer Here >>

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

<< ADD Answer Here >>

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

<< ADD Answer Here >>

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

<< ADD Answer Here >>

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

<< ADD Answer Here >>

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

<< ADD Answer Here >>

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?

<< ADD Answer Here >>

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

<< ADD Answer Here >>

9.3 What design choices were made to enhance privacy?

<< ADD Answer Here >>

Conclusion

The concluding section should inform the reader, in summary fashion, how you constructed your system, program, rule, or technology based on privacy risks and mitigation strategies.

<< ADD Conclusion Here >>

Responsible Officials

<< ADD Privacy Officer/Project Manager>>

Department of Homeland Security

Approval Signature Page

_____ <<Sign Date>>

Maureen Cooney
Acting Chief Privacy Officer
Department of Homeland Security