Privacy Impact Assessment
for the

<<ADD SYSTEM NAME>>

<<ADD Publication Date>>

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

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

Abstract

The abstract should be a minimum of three sentences and a maximum of four, if necessary, and conform to the following format:

- First sentence should be the name of the component and system.

- Second sentence should be a brief description of the system and its function.

- Third sentence should explain why the PIA is being conducted.

<< ADD Abstract Here >>

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

- The system name and the name of the Department component(s) who own(s) the system;

- The purpose of the program, system, or technology and how it relates to the component's and Department's mission;

- A general description of the information in the system;

- A description of a typical transaction conducted on the system;

- Any information sharing conducted by the program or system;

- A general description of the modules and subsystems, where relevant, and their functions; and

- A citation to the legal authority to operate the program or system.

<< ADD Introduction Here >>

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?

<< ADD Answer Here >>

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

<< ADD Answer Here >>

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

<< ADD Answer Here >>

1.4   How is the information collected?

<<ADD Answer Here>>

1.5   How will the information be checked for accuracy?

<< ADD Answer Here >>

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

<< ADD Answer Here >>

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

<< ADD Answer Here >>

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.

<< ADD Answer Here >>

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

<< ADD Answer Here >>

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

<< ADD Answer Here >>

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.

<< 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 information is retained?

<< ADD Answer Here >>

3.2 How long is information retained?

<< ADD Answer Here >>

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

<< ADD Answer Here >>

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

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

<< ADD Answer Here >>

4.2 How is the information transmitted or disclosed?

<< ADD Answer Here >>

4.3 <u>Privacy Impact Analysis</u>: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing 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 organization(s) is the information shared, what information is shared, and for what purpose?

<< ADD Answer Here >>

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.

<< ADD Answer Here >>

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

<< ADD Answer Here >>

5.4 <u>Privacy Impact Analysis</u>**: Given the external sharing, explain the privacy risks 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?

<< ADD Answer Here >>

6.2 Do individuals have the 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? If so, how does the individual exercise the right?

<< ADD Answer Here >>

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

<< ADD Answer Here >>

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?

<< ADD Answer Here >>

7.2 What are the procedures for correcting inaccurate or 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 formal redress is provided, what alternatives are available to the individual?

<< ADD Answer Here >>

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

<< ADD Answer Here >>

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?

<< ADD Answer Here >>

8.2 Will Department contractors have access to the system?

<< ADD Answer Here >>

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

<< ADD Answer Here >>

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

<< ADD Answer Here >>

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

<< ADD Answer Here >>

8.6   <u>Privacy Impact Analysis</u>: 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?

<< 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   What type of project is the program or system?

<< ADD Answer Here >>

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

<< ADD Answer Here >>

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

<< ADD Answer Here >>

Approval Signature Page

_____

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security