



Commandant
United States Coast Guard

2100 Second Street, S.W.
Washington, DC 20593-0001
Staff Symbol: CG-611
Phone: (202) 267-2327
Fax: (202) 267-1123
anjohanson@comdt.uscg.mil

COMDTINST 5260.4A
NOV 9 2005

COMMANDANT INSTRUCTION 5260.4A

Subj: COAST GUARD PRIVACY IMPACT ASSESSMENT (PIA)

Ref: (a) The Coast Guard Freedom of Information and Privacy Acts Manual, COMDTINST M5260.3 (series)
(b) Homeland Security Act of 2002
(c) E-Gov Act of 2002

1. PURPOSE. This Instruction implements the Department of Homeland Security (DHS) policy governing Privacy Impact Assessments (PIA) (enclosure (1)), and establishes the authority, roles, and responsibilities for PIAs during the system development process. It further implements the requirements of the E-Government and Department of Homeland Security Acts of 2002.
2. ACTION. Area and district commanders, commanders of maintenance and logistics commands, commanding officers of Headquarters units, assistant commandants for directorates, Judge Advocate General, and special staff offices at Headquarters shall ensure that all Coast Guard and contractor support personnel or organizations involved in systems development comply with the provisions of this Instruction. Internet release authorized.
3. DIRECTIVES AFFECTED. Coast Guard Privacy Impact Assessment (PIA), Commandant Instruction 5260.4 is cancelled.
4. DISCUSSION. PIAs are necessary to ensure that the voluminous amount of data collected on individuals is properly secured. While this policy specifically targets the systems development process, it applies to all systems used to gather personal privacy data on private citizens, government employees, and contracting personnel. The public has an inherent right to expect that the Coast Guard will collect, maintain, use, and disseminate personally identifiable

DISTRIBUTION – SDL No. 143

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A																										
B	45	5	5	1	1	1	1	1	1	1	1	1	10	1	1	10	1	1	1	2	2	2	2	2	5	1
C			1			1	1			1	3			1												
D																										
E				1				1		1				1	1								1			
F																	1	1	1							
G																										
H																										

NON-STANDARD DISTRIBUTION:

information (PII) and data only as authorized by law and as necessary to carry out its mission. Requiring PIAs is intended to make systems development a multidisciplinary effort, involving systems owners, IT specialists, security, and privacy experts. The primary purpose of a PIA is to allow the organization building or operating a system that collects, maintains, and disseminates PII to determine whether it is in compliance with relevant data protection legislation at any particular stage. DHS published "Privacy Impact Assessments - Official Guidance," (enclosure (1)), to guide system owners and developers in assessing privacy concerns during the early stages of systems development or major modifications. This guide shall be followed to determine if a PIA is required for your system(s). If required, respond to the questions in accordance with enclosure (1) of this Instruction. Additionally, provide the contact information by completing enclosure (2). Send enclosures (1) and (2) to Commandant (CG-611). Following approval, DHS will submit for publication in the Federal Register. The PIA Process Flow Chart (enclosure 3), is provided for information purposes.

5. BACKGROUND. The Office of Management and Budget (OMB) guidance to agencies on implementing the privacy provisions of Section 208 of the E-Government Act of 2002 (Public Law 107-347, 44 U.S.C. Ch 36) includes a requirement for PIAs. In addition to existing policies contained in reference (a), agencies are required to conduct PIAs for electronic information systems or projects that collect, maintain, or disseminate information in identifiable form from or about members of the public. Significantly altered IT systems are subject to assessment as well. Agencies must make these assessments publicly available. Failure to complete a PIA could possibly jeopardize funding by OMB. With the increased volume of data collected from public citizens, there is an expectation that privacy data be maintained in a secure manner.
6. OTHER RELATED LEGISLATION.
 - a. The Privacy Act of 1974, as Amended (5 U.S.C. 552a) affords individuals the right to privacy in records that are maintained and used by Federal agencies. The Act includes the Computer Matching and Privacy Protection Act of 1998 (Public Law 100-503).
<http://www.usdoj.gov/04foia/privstat.htm>.
 - b. Freedom of Information Act of 1966 as Amended (5 U.S.C. 552) establishes a presumption that records in the possession of agencies and departments of the Executive Branch of the United States Government are accessible to the people.
<http://www.usdoj.gov/04foia/foiastat.htm>
 - c. Reference (b), Homeland Security Act of 2002 (H.R. 5005 Section Subtitle C-Information Security), http://www.whitehouse.gov/deptofhomeland/hr_5005_enr.pdf, establishes that a PIA of proposed rules on the privacy of personal information, including the type of PII collected and the number of people affected must be completed. An annual report to Congress is prepared on the activities that affect privacy, including complaints of privacy violations, implementation of the Privacy Act of 1974, internal controls, and other matters.
 - d. Reference (c), E-gov Act of 2002, Section 208, (Public Law 107-347, 44 U.S.C. Ch 36), <http://www.whitehouse.gov/omb/memoranda/m03-22.html#a>, provides guidance on implementing the privacy provisions. This guidance directs agencies to conduct assessments

before developing or procuring an information system, or initiating a new collection of PII that will be processed electronically.

7. CHANGES.

- a. PIAs are required for both internal and external IT systems.
- b. PIAs are required for new or updated Rulemaking proposals that impact PII. If an organization decides to collect new information or update its existing collections as part of a rulemaking, a PIA is required. The PIA should discuss how the management of these new collections ensures conformity with privacy law. Even if a program has specific authority to collect certain information or build a certain program, a PIA is required.
- c. A PIA should be conducted for all systems, including those that are classified. For such systems, the requirement to publish may be exempt and all proper redactions will be made prior to any public release by DHS.
- d. In some instances, an organization may choose to develop a “Negative PIA.” A Negative PIA documents why a full PIA is not necessary. For example, if the system does not collect PII, a short negative PIA will demonstrate that a traditional PIA is not required. This is particularly useful for major budget submissions, so that decisions made by the Privacy Office and the component are memorialized for subsequent budget submissions.
- e. Additional Questions:
 - (1) What specific legal authorities, arrangements, and/or agreements define the collection of information?
 - (2) Has the retention schedule been approved by the National Archives and Records Administration (NARA)? If so, what is the name of the Record Schedule?
 - (3) With which internal or external organization(s) is the information shared? For each organization, what information is shared and for what purposes?
 - (4) How is the information transmitted or disclosed?
 - (5) Was notice provided to the individual prior to the collection of information? If yes, please provide a copy of the notice.
 - (6) 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 the PIA.
 - (7) Is the data secured in accordance with the Federal Information Security Management Act (FISMA) requirements? If yes, when was Certification & Accreditation last completed?
 - (8) Were competing technologies evaluated to assess and compare their ability to effectively achieve system goals?

- (9) Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system?
 - (10) Does the PIA cover a new, significantly modified, or legacy system? Specify.
 - (11) Who will be responsible for protecting privacy rights in the system?
8. ENVIRONMENTAL ASPECT AND IMPACT CONSIDERATIONS. Environmental considerations were examined in the development of this Instruction and are not applicable.
9. FORMS. Privacy Impact Assessment Contact Information, CGHQ-6050 is available in USCG Electronic Forms on the Standard Workstation or on the Internet at <http://www.uscg.mil/ccs/cit/cim/forms1/welcome.htm> or the Intranet at <http://cgweb.uscg.mil/g-c/g-ccs/g-cit/g-cim/forms1/main.asp>.

R. T. HEWITT /s/
Assistant Commandant for Command, Control,
Communications, Computers, and Information Technology

Encl: (1) DHS Privacy Impact Assessments Official Guidance
(2) PIA Contact Information
(3) PIA Flow Chart



Privacy Impact Assessments

Official Guidance

The Privacy Office

Effective July 2005



**Homeland
Security**



“Privacy is a value that must be embedded in the very culture and structure of the organization. I know that we can and will succeed in this – because our leadership and our employees believe in and act on this value – for themselves, their neighbors, and their families – each day.”

Maureen Cooney
Acting Chief Privacy Officer
U.S. Department of Homeland Security

DHS Privacy Office Compliance

Maureen Cooney
Acting Chief Privacy Officer
Chief of Staff, Privacy Office and Senior Advisor International Privacy Programs

Elizabeth Withnell
Chief Counsel, Privacy Office

Rebecca Richards
Director, Privacy Compliance

Nathan Coleman
Privacy Analyst

Privacy Impact Assessments

The Privacy Office Official Guidance

Effective July 2005

Contents

7	Introduction
8	What is a PIA?
8	Complying
10	Information Covered
12	When to Conduct a PIA
13	How to Conduct a PIA
17	Writing the PIA
29	Contact the Privacy Office
31	PIA Triggers

Introduction

Privacy Impact Assessments (“PIAs”) are required by Section 208 of the E-Government Act for all Federal government agencies that develop or procure new technology involving the collection, maintenance or dissemination of personally identifiable information or that make substantial changes to existing technology for managing information in identifiable form. The Office of Management and Budget ensures that PIAs necessitated under the E-Government Act are completed by requiring them as part of the annual budget process.

The Chief Privacy Officer of the Department of Homeland Security is required by Section 222 of the Homeland Security Act to assure that the technology used by the Department sustains privacy protections. The PIA for new technology, systems, and programs is the mechanism by which the Chief Privacy Officer conducts this assessment. In addition, the Chief Privacy Officer is required to conduct PIAs for proposed rulemakings of the Department. The Chief Privacy Officer approves PIAs conducted by DHS offices and programs.

In 2004, the DHS Privacy Office issued “Privacy Impact Assessments Made Simple.” This amended guidance supersedes “PIAs Made Simple,” and reflects the requirements of both Section 208 of the E-Government Act of 2002 and Section 222 of the Homeland Security Act of 2002. The DHS Chief Privacy Officer requires that all new PIAs follow this guidance after the publication date of this guidance.

What is a PIA?

A PIA is an analysis of how personally identifiable information is collected, stored, protected, shared and managed. “Personally identifiable information” is defined as information in a system or online collection that directly or indirectly identifies an individual whether the individual is a U.S. Citizen, Legal Permanent Resident, or a visitor to the U.S. In some cases, personal information, such as a body scan, may be captured only for a short period of time. This still is considered a collection, however, and a PIA would need to be conducted during the development and prior to the deployment of the new technology.

The purpose of a PIA is to demonstrate that system owners and developers have consciously incorporated privacy protections throughout the entire life cycle of a system. This involves making certain that privacy protections are built into the system from the start, not after the fact when they can be far more costly or could affect the viability of the project.

The PIA process requires that candid and forthcoming communications occur between the program manager and the Privacy Office to ensure appropriate and timely handling of privacy concerns. Addressing privacy issues publicly builds citizen trust in the mission of the Department of Homeland Security.

Complying with the PIA Requirement

The Department of Homeland Security is committed to analyzing and sharing information and intelligence through all of its agencies so that the urgent task of protecting the homeland can be carried out. At the same time, the Department should have in place robust protections for the privacy of any personal information that we collect, store, retrieve and share.

These protections, embodied in Federal law, seek to foster three concurrent objectives:

- Minimize intrusiveness into the lives of individuals;
- Maximize fairness in institutional decisions made about individuals; and
- Provide individuals with legitimate, enforceable expectations of confidentiality.

Federal law recognizes the ever-increasing amount of information stored in government systems and the speed with which computers can process and transfer data. The E-Government Act of 2002 mandates an assessment of the privacy impact of any substantially revised or new information technology system because of the potential privacy impacts from maintenance of electronic databases. Similarly, the Homeland Security Act of 2002 acknowledges the Department's role in collecting sensitive information about individuals and includes a requirement that the Chief Privacy Officer of DHS assure that technology used by the Department sustains privacy protections. The Homeland Security Act also recognizes the potential effect of proposed rules on privacy and authorizes the Chief Privacy Officer to conduct privacy impact assessments on proposed rules of the Department.

The document in which the Department memorializes its compliance with the E-Government Act and Homeland Security Act is called a "Privacy Impact Assessment," or "PIA." A PIA analyzes how personal information is collected, used, stored, and protected by the Department and examines how the Department has incorporated privacy concerns throughout its development, design and deployment of the technology and/or rulemaking.

The PIA is a document that helps the public understand what information the Department is collecting, why the information is being collected, how the information will be used and shared, how the information may be accessed, and how it will be stored. This document builds trust between the public and the Department by increasing transparency of the Department's systems and goals.

The PIA demonstrates that the Department considers privacy from the beginning stages of a system's development and throughout the system's life cycle. The PIA process and the document itself are intended to ensure that privacy protections are built into the system from the start, not after the fact when privacy concerns can be far more costly to address or could affect the viability of the project. Additionally, the PIA demonstrates that the system developers and owners have made technology choices that reflect the incorporation of privacy into the fundamental system architecture. In order to make the PIA comprehensive and meaningful, it should involve collaboration between program experts, information technology experts, security experts, and privacy experts.

The PIA is a living document that needs to be updated regularly as the program and system are developed, not just when the system is deployed. In cases where a legacy system is being updated the PIA demonstrates that the system developers and program managers have implemented privacy protections into the updates. The PIA for legacy systems making changes that affect

privacy, the document may be longer than new programs with existing PIAs that need only update the PIA.

Under the E-Government Act, a PIA should accomplish two goals: (1) It should determine the risks and effects of collecting, maintaining and disseminating information in identifiable form via an electronic information system; and (2) It should evaluate protections and alternative processes for handling information to mitigate potential privacy risks. The Office of Management and Budget (OMB) oversees the implementation of these goals by requiring PIAs to be submitted as part of the annual budget process for all new technologies or existing technologies that are being updated.

Under the Homeland Security Act of 2002, the Chief Privacy Officer is charged with ensuring that the Department uses technologies that sustain and do not erode privacy. Part of this charge is fulfilled by requiring that agencies complete PIAs for all new technologies, new collections of personal information, and new systems or existing systems that are being substantially updated. The statute also requires that agencies conduct PIAs on all new rulemakings that could impact privacy. By following this guidance, the PIA requirement will be fulfilled.

Information Covered by the PIA

A PIA should be completed for any system, program, technology or rulemaking that involves personally identifiable information. Personally identifiable information is information in a system, online collection, or technology: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. As found in OMB Memorandum M-03-22, these data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors. In some cases a system or technology may only momentarily collect information about an individual, such as a surveillance camera. A PIA is required for the acquisition of such a new technology. In other cases, the technology may not be changing, but a program decides to use data from a new source such as commercial aggregator of information.

Examples of personally identifiable information include: name, date of birth, mailing address, telephone number, social security number, e-mail address, zip code, address, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), internet protocol addresses, biometric identifiers, photographic facial images, any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify an individual.

Examples of technology with privacy implications: In some cases the technology may only collect personal information for a moment. For example, a body screening device may capture the full scan of an individual, while the information may not be maintained for later use, the initial scan may raise privacy concerns and a PIA would be required.

Examples of new data collections with privacy implications: Commercial data aggregators may provide consolidated data bases of public information that a program uses to check the last

known address of a suspected Visa violator. In some cases the program may choose to “ping” the database of the data aggregator rather than download extensive information. No matter how a program decides to incorporate the use of a commercial data aggregator, a PIA would be required.

Regarding “Private” Information

Personally identifying information should not be confused with “private” information. Private information is information that an individual would prefer not be known to the public because it is of an intimate nature. Personally identifying information is much broader; it is information that identifies a person or can be used in conjunction with other information to identify a person, regardless of whether a person would want it disclosed. If the information or collection of information connects to an individual, it is classified as “personal information.”

Example: A license plate number is personally identifying information because it indirectly identifies an individual, but it is not deemed “private” because it is visible to the public. PIAs require analysis of the broader “personally identifiable information,” not just the narrower “private information.”

Regarding Privacy Act System of Records Notice (SORN) requirements v. PIA requirements

The Privacy Act requires agencies to publish Systems of Records Notices (SORNs) that describe the categories of personally identifiable information that they collect, maintain and use. Generally, the requirements to conduct a PIA are broader and more frequent than the requirements for System of Records Notices. The PIA requirement is triggered by both the technology and the collection of information. Even if the collection of information remains the same and is already covered by an existing SORN, if the technology using the information is changing, the PIA must be completed or updated to reflect the new impact of the technology. The PIA requirement does not provide an exemption for pilot testing programs. If the system is being designed to handle personal information even in a pilot test, the PIA is required to be published prior to the commencement of any pilot test. If in the process of developing a new program, a SORN needs to be updated, a PIA will also be required.

When to Conduct a PIA

A PIA should be conducted when an office is doing any of the following:

- Developing or procuring any new technologies or systems that handle or collect personal information. A PIA is required for all budget submissions to OMB. The PIA should show that privacy was considered from the beginning stage of system development. If a program is beginning with a pilot test, a PIA is required prior to the commencement of the pilot test – even if real personal information is not going to be used in the pilot test.

- Developing system revisions. If an organization modifies an existing system, a PIA will be required. For example if a program adds additional sharing of information either with another agency or incorporating commercial data from an outside data aggregator, a PIA is required. Appendix I of this document provides extensive examples.
- Issuing a new or updated rulemaking that affects personal information. If an organization decides to collect new information or update its existing collections as part of a rulemaking, a PIA is required. The PIA should discuss how the management of these new collections ensures conformity with privacy law. Even if a program has specific authority to collect certain information or build a certain program, a PIA is required.

Classified Information and Systems

A PIA should be conducted for all systems, including classified systems, but the program may be exempted from the requirement to publish the PIA. Note that Privacy Office personnel are cleared to read classified materials, and prior to public release of any PIA, all proper redactions will be made.

Negative PIAs

In some instances, an organization may choose to develop a negative PIA. A negative PIA documents why a full PIA is not necessary. For example, if the system does not collect personally identifiable information, a short negative PIA will demonstrate that a traditional PIA is not required. This is particularly useful for major budget submissions, so that decisions made by the Privacy Office and the component are memorialized for subsequent budget submissions.

How to Conduct a PIA

Section 208 of the E-Government Act of 2002 states that agencies are required to conduct PIAs for electronic information systems and collections. The Act requires agencies to make PIAs publicly available. PIAs should be clear, unambiguous, and understandable to the general public.

The length and breadth of a PIA will vary by the size and complexity of the system. Any new system development that has major budget implications or involves the processing of personal information should be able to demonstrate, through the PIA, that an in-depth analysis was done to ensure that privacy protections were built into the system.

In order to give DHS PIAs a consistent look and feel, documents should be provided in Times New Roman, 12 point font with 1" margins. All PIAs done after the effective date of this amended guidance should be in the format outlined below. All questions should be answered. If a particular question is not applicable, please state that it is not applicable and the justification.

Please adhere to the following guidelines when drafting a PIA:

- Draft PIAs from the perspective of a member of the public who knows nothing about the system or the technology.

- Spell out each acronym the first time you use it in the document. For example: Department of Homeland Security (DHS).
- Use words, phrases, or names in the PIA that are readily known to the average person.
- Technical terms or references should be defined.
- Clearly reference projects and systems and provide explanations, if needed, to aide the general public.
- References to National Institute of Science and Technology (NIST) publications and other documents should include the complete name of the reference (e.g., NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems. Subsequent references may use the abbreviated format. Full names for NIST documents can be found at <http://csrc.nist.gov/publications/nistpubs/>.

Writing the PIA

Guide to the Template for a Privacy Impact Assessment

Writing the PIA

In a separate document a template has been developed for ease of use, which includes only the top level questions noted below. The sublevel questions and examples in the below outline are to provide you with additional guidance to aide in responding to the required questions.

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.

Section 1.0 The system and the information collected and stored with the system.

The following questions are intended to define the scope of the information requested and/or collected 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?

1.1.1 Identify and list all personal information that is collected and stored in the system. This

could include, but is not limited to, name, date of birth, mailing address, telephone number, social security number, e-mail address, zip code address, facsimile number, medical record number, bank account number, health plan beneficiary number, any other account numbers, certificate/license number, vehicle identifier including license plate, marriage record, civil or criminal history information, device identifiers and serial number, uniform resource locators (URLs), education record, internet protocol addresses, biometric identifiers, photographic facial image, or any other unique identifying number or characteristic.

- 1.1.2** In some cases, a general summary of the information may be put in the first section and an appendix with the full list may be added to the back of the PIA.

1.2 From whom is the information collected?

- 1.2.1** List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from another source, such as commercial data aggregators.

- 1.2.2** Describe why information from sources other than the individual are required. For example, if a program is using data from a commercial aggregator of information, state the fact that this is where the information is coming from and the in 1.3 indicate why the program is using this source of data.

1.3 Why is the information being collected?

- 1.3.1** In responding to this question, you should include:

1.3.1.1 A statement of why this PARTICULAR personally identifiable information that is collected and stored in the system is necessary to the component's or to DHS's mission. Merely stating the general purpose of the system without explaining why particular types of personally identifiable information should be collected and stored is not an adequate response to this question.

1.3.1.2 For example, a statement that a system may collect name, date of birth and biometrics in order to verify an individual's identity at the border is adequately specific. However, stating that the above information will be collected to ensure border security is not sufficient. It would be more appropriate to state that the information is collected to compare to the terrorist watch list.

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

Privacy Impact Analysis: Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated. For example, if during the design process, a decision was made to collect less data, include a discussion of this decision.

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 uses of the information.

2.1.1 Identify and list each use (internal and external to DHS) of the information collected or maintained.

2.1.2 If a SORN has been published for the system, the routine uses from the SORN should be described in this section. In addition, list the uses internal to DHS since the routine uses listed in the SORN are limited to disclosures made outside of DHS.

2.1.3 Do not list the routine uses directly from the SORN, summarize the most relevant ones. For example, if the system does not regularly handle requests from Congressional members, this does not need to be included in the summary. If instead, the system provides full access to another agency for their use of the information, this should be discussed in this section.

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

2.2.1 Many systems sift through large amounts of information in response to a user inquiry or programmed functions. This is loosely known as data mining. When these systems sift through information they make determinations and, sometimes, conclusions based upon the information they analyze. If the system being analyzed in the PIA conducts such preliminary and conclusory functions, please provide greater detail on what type of determinations the system makes.

2.2.2 If the system creates or makes available new or previously unavailable information about an individual, state/explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to government employees who make determinations about the individual? If so, explain fully under what circumstances that information will be used and by whom.

2.3 How will the information collected from individuals or derived by the system, including the system itself be checked for accuracy? In responding to this question address the following where applicable:

2.3.1 Explain whether information in the system is checked against any other source of information (within or outside your organizational entity) before the information is used to make decisions about an individual. If not, explain whether your organization has any other rules or procedures in place to reduce the instances in which inaccurate data is

stored in the system.

- 2.3.2** If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

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. For example, are audit logs regularly reviewed to ensure appropriate use of information? Are strict disciplinary programs in place if an individual is found to be inappropriately using the information?

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

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

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?
- 4.1.1** The term “internal” references components, agencies, and any other organization within DHS. This question is directed at the intra-departmental sharing of information within DHS.
- 4.1.2** Identify and list the name(s) of any components, agencies and any other organizations within DHS with which the information is shared.
- 4.2** For each organization, what information is shared and for what purpose?
- 4.2.1** Is the information shared in bulk or does the organization have direct access to the information?
- 4.2.2** If you have specific authority to share the information, please provide a citation to such authority.

4.2.3 For each interface with a system outside your component, state what specific information is shared with the specific components, agencies, and any other organizations within DHS.

4.3 How is the information transmitted or disclosed?

4.3.1 Describe how the information is transmitted to each component, agency, and any other organization within DHS. For example is the information transmitted electronically, by paper, or by some other means?

Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated. For example, if a decision was made to limit internal sharing to certain components because of privacy or other concerns, include such a discussion.

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?

5.1.1 The term “external” references other departments, agencies and organizations that are not a part of DHS. This could be other Departments, law enforcement and intelligence agencies, the private sector, and state and local entities. This question is directed at inter-departmental sharing, as well as with private entity and state or local information sharing.

5.1.2 Identify and list the name or names of the federal, state, or local government agency or private sector organization with which the information is shared.

5.2 What information is shared and for what purpose?

5.2.1 For each interface with a system outside DHS, state what specific information is shared with each specific partner. For example, Customs and Border Protection may share its information on an individual with the FBI.

5.2.2 Where you have a specific authority to share the information, please provide a citation to the authority.

5.3 How is the information transmitted or disclosed?

5.3.1 Is the information shared in bulk or does the organization have direct access to the information?

- 5.3.2** Describe how the information is transmitted to entities external to DHS and whether it is transmitted electronically, by paper, or some other means.
- 5.3.3** Describe how the information arrives from entities external to DHS and whether it is transmitted electronically, by paper, or some other means.
- 5.4** Is a Memorandum of Understanding (MOU), contract, or agreement in place with any external organization(s) with whom information is shared, and does the MOU reflect the scope of the information currently shared?
 - 5.4.1** If an MOU is not in place, is the sharing covered by a routine use in the System of Records Notice? If not, explain the steps being taken to address this omission.
- 5.5** How is the shared information secured by the recipient?
 - 5.5.1** For each interface with a system outside DHS:
 - 5.5.1.1** Identify and list who is responsible for assuring the security and privacy of the data once it is shared; and if possible, include a reference to and quotation from any MOU, contract, or other agreement that defines the parameters of the sharing agreement.
 - 5.5.1.2** Explain whether the external system has a certification & accreditation (C & A) under FISMA or other relevant computer security standards. If the external system has not completed C & A, how have the external system's security issues been addressed to ensure the privacy and security of the information once it is shared?
- 5.6** What type of training is required for users from agencies outside DHS prior to receiving access to the information?

Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated. For example, if a decision was made to limit external sharing, include such a discussion.

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 the collection of information? If yes, please provide a copy of the notice. 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, explain why not.
 - 6.1.1** Question 6.1 is directed at the notice provided prior to collection of the information. This refers to whether the person is aware that his or her information is being collected.

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

6.2.1 Question 6.2 is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached.

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

6.3.1 Question 6.3 is directed at whether the consent given to the collection of information covers all uses (current or potential) of their information or if an individual may provide consent for specific uses. If such consent is required, how would the individual consent to each use.

Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them. For example, if previously no notice was provided to the individual about how to correct information and subsequently the program decided to provide this information, include a discussion of this decision.

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 that allow individuals to gain access to their own information?

7.1.1 Cite any procedures or regulations your component has in place that allow access to information. These would be in addition to the DHS FOIA/Privacy Act regulations. For example, if your component has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section, in addition to DHS procedures.

7.1.2 If the system is exempt from the amendment/correction provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found.

7.1.3 If the system is not a Privacy Act system, please explain what procedures and/or regulations are in place that cover an individual gaining access to his/her own information.

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

7.2.1 Discuss the procedures and provide contact information for the appropriate person to whom such issues should be addressed.

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

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

7.4.1 Redress is the process by which an individual gains access to his/her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and/or Freedom of Information Act (FOIA).

Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974 as well as in the Freedom of Information Act, what procedural rights are provided and, if access, correction, and redress rights are not provided, please explain why not.

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?

8.1.1 Identify and list the types of users. For example: managers, system administrators, contractors, and developers may have access to the system.

8.1.2 Identify users from other agencies that may have access to the system and under what roles do these individuals have access to the system.

8.2 Will contractors to DHS have access to the system?

8.2.1 If so, please submit a copy of the contract describing their role to the Privacy Office with this PIA.

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

8.3.1 Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have “read-only” access while others may be able to make certain amendments or changes to the information.

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

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

8.5.1 For example, when an employee no longer works for the organization or in a specific job function, there is a set procedure for removing access in timely.

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

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

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

Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how you mitigated them. For example, if a decision was made to tighten access controls by restricting access to specific users, include such a discussion.

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 Were competing technologies evaluated to assess and compare their ability to effectively achieve system goals?

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

9.3 What design choices were made to enhance privacy?

Conclusion

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

Approval and Signature Page

Provide a contact name and number for the privacy officer or program manager of the program covered by this PIA, as well as a place for the Chief Privacy Officer to sign the final PIA when it is completed and approved.

Questions? Contact Us.

Privacy Office

U.S. Department of Homeland Security

Arlington, VA 22202

Email: pia@dhs.gov

Phone: 571-227-3813

Web Site Link: www.dhs.gov/privacy

Appendix I PIA Triggers

Please consult with the Privacy Office to determine whether a PIA is required and to identify any existing PIAs or System of Records Notices (SORNs). According to OMB Memorandum M-03-22, the system activities listed below may require a PIA:

Conversions

When converting paper-based records to electronic systems;

Anonymous to Non-Anonymous

When functions applied to an existing information collection change anonymous information into information in identifiable form;

Significant System Management Changes

When new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system:

For example, when an agency employs new relational database technologies or web-based processing to access multiple data stores, such additions could create a more open environment and avenues for exposure of data that previously did not exist.

Significant Merging

When agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated:

For example, when databases are merged to create one central source of information, such a link may aggregate data in ways that create privacy concerns not previously at issue.

New Public Access

When user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public;

Commercial Sources

When agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources. (Merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement);

New Interagency Uses

When agencies work together on shared functions involving significant new uses or exchanges

of information in identifiable form, such as the cross-cutting E-Government initiatives; in such cases, the lead agency should prepare the PIA;

Internal Flow or Collection

When alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form;

Alteration in Character of Data

When new information in identifiable form added to a collection raises the risks to personal privacy.

For example, the addition of health or financial information may lead to additional privacy concerns that otherwise would not arise.

Privacy Office Staff

Maureen Cooney

Chief Privacy Officer, Acting
Chief of Staff and Senior Advisor, International Privacy

Sandra L. Hawkins

Administrative Officer

Elizabeth Withnell

Chief Counsel to the

Toby Milgrom Levin

Senior Advisor

Tony Kendrick

Director, Departmental Disclosure

John Kropf

Director, International Privacy Programs

Rebecca Richards

Director, Privacy Compliance

Peter Sand

Director, Privacy Technology

Catherine Papoi

Deputy Director, Departmental Disclosure

Lane Raffray

Privacy Policy Analyst

Kenneth P. Mortensen

Senior Privacy Advisor

Anna Slomovic

Senior Privacy Analyst

Nathan Coleman

Privacy Analyst

Robyn Kaplan

Privacy Analyst

Sandra Debnam

Administrative Assistant

Doug McComb

FOIA Specialist

Sarah Mehlhaff

FOIA Specialist

Dan Stein

FOIA Specialist

Component Privacy Officers

Lisa Dean

Privacy Officer, TSA

Elizabeth Gaffin

Privacy Officer, CIS

Andy Purdy

Privacy Officer, IAIP NCSD

Steve Yonkers

Privacy Officer, US-VISIT



Privacy Impact Assessment
for the

<<SYSTEM NAME>>

<<Publication Date>>

Contact Point

<<Contact Person>>

<<Program/Agency/Office>>

<<Component/Directorate>>

<<Contact Phone>>

Reviewing Official

Maureen Cooney

Acting Chief Privacy Officer

Department of Homeland Security

(571) 227-3813

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.

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?**
- 1.2 From whom is information collected?**
- 1.3 Why is the information being collected?**
- 1.4 What specific legal authorities/arrangements/agreements define the collection of information?**

Privacy Impact Analysis: Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated. For example, if during the design process, a decision was made to collect less data, include a discussion of this decision.

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.**
- 2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern (Sometimes referred to as data mining)?**
- 2.3 How will the information collected from individuals or derived from the system be checked for accuracy?**

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. For example, are audit logs regularly reviewed to ensure appropriate use of information? Are strict disciplinary programs in place if an individual is found to be inappropriately using the information?

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

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

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?**

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

4.3 How is the information transmitted or disclosed?

Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated. For example, if a decision was made to limit internal sharing to certain components because of privacy or other concerns, include such a discussion.

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?

5.2 What information is shared and for what purpose?

5.3 How is the information transmitted or disclosed?

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?

5.5 How is the shared information secured by the recipient?

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

Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated. For example, if a decision was made to limit external sharing, include such a discussion.

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

Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them. For example, if previously no notice was provided to the individual about how to correct information and you subsequently decided to provide this information, include a discussion of this decision.

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?**
- 7.2 What are the procedures for correcting erroneous information?**
- 7.3 How are individuals notified of the procedures for correcting their information?**

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

Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, what procedural rights are provided and, if access, correction and redress rights are not provided please explain why not.

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? (For example, program managers, IT specialists, and analysts will have general access to the system and registered users from the public will have limited access.)**
- 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.**
- 8.3 Does the system use “roles” to assign privileges to users of the system?**
- 8.4 What procedures are in place to determine which users may access the system and are they documented?**
- 8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?**
- 8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?**
- 8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?**
- 8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?**

Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated. For example, if a decision was made to tighten access controls by restricting access to specific users, include such a discussion.

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?**

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

- 9.3 What design choices were made to enhance privacy?**

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.

Responsible Officials

<<Privacy Officer/Project Manager>>

Department of Homeland Security

Approval Signature Page

_____ <<Sign Date>>

Maureen Cooney
Acting Chief Privacy Officer
Department of Homeland Security

U.S. Department of Homeland Security U.S. Coast Guard CGHQ-6050 Rev. (07-04)		Privacy Impact Assessment Contact Information	
Name of the System			
Signature of Assessor <i>(i.e., System Owner, Operator, Developer, or Other)</i>		Date	
Print Name		Title/Position	
Signature of Program Manager <i>(if not Assessor)</i>		Date	
Print Name		Title/Position	
Agency and Office/Department			
Street Address			
City, State and Zip Code			
Phone Number	Fax Number	E-mail Address	

Please Return Completed Form To CG-611, Room 6106

FOR COMMANDANT, CG-611 USE ONLY

Reviewed By	Date	Approved By	Date
Comments			

Reset

Privacy Impact Assessment (PIA) Process

The purpose of a PIA is to document – at the very earliest stage of a project – how new or revised IT systems have privacy built into the fundamental architecture of the system, including technology choices.

