



COMDTINST 5260.4
Sep 23 2004

COMMANDANT INSTRUCTION 5260.4

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 policy governing Privacy Impact Assessments (PIA) as indicated in 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 of the Coast Guard, and special staff offices at Headquarters shall ensure that all Coast Guard and contractor support personnel or organizations involved in the systems development comply with the provisions of this Instruction. Internet release authorized.
3. DIRECTIVES AFFECTED. Chapter 12 of reference (a) will be modified to incorporate PIA requirements.
4. DISCUSSION. Privacy impact assessments 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 identifiable personal information and data only as authorized by law and as necessary to carry out its mission. Requiring

DISTRIBUTION – SDL No. 141

	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	2	2	2		2	2	2	2	1	1		1	1	1	11	1	1	1	1		1					
B	1	8	20*	1	12	3	10	10	3	10	3	3	2	10	1	2	2	25	1	2	2	1	3	1	1	1
C	3	2	1	3	1	1	1	1	11		3	1	2	2	25		1	1	3	1	1	1	1	2	1	1
D	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1		1	1	1			1
E	1	2						1		1	1	1		1	1		1		1	1			1	21		
F																	1	1	1							
G	1	1	1	1	1																					
H																										

NON-STANDARD DISTRIBUTION:

PIAs is intended to make systems development a multidisciplinary effort, involving systems owners, IT specialists, and security and privacy experts. The primary purpose of a privacy impact assessment is to allow the organization building or operating a system that collects, maintains and disseminates personal information to decide whether it is in compliance with relevant data protection legislation at any particular stage.

5. BACKGROUND. The Office of Management and Budget (OMB)'s 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 privacy impact assessments. In addition to existing policies contained in reference (a), agencies are required to conduct privacy impact assessments 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 the privacy data will be maintained in a secure manner, and that agencies seriously consider the approach they will take to incorporate information security in their business cases for major IT projects.
6. OTHER RELATED LEGISLATION.
 - a. Privacy Act of 1974, as Amended (5 USC 552a) affords individuals the right to privacy in records that are maintained and used by Federal agencies. 5 USC 552a includes the Computer Matching and Privacy Act of 1998 (Public Law 100-503).
<http://www.usdoj.gov/04foia/privstat.htm>
 - b. Freedom of Information Act of 1966 as Amended (5 USC 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. 50005 Section Subtitle C-Information Security), http://www.whitehouse.gov/deptofhomeland/hr_5005_enr.pdf, establishes that a privacy impact assessment of proposed rules on the privacy of personal information, including the type of personal information 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 USC, Change 36), http://www.whitehouse.gov/omb/egov/pres_state2.htm, provides guidance on implementing the privacy provisions. This guidance directs agencies to conduct reviews of how information about individuals is handled within their agency when they use Information Technology (IT) to collect new information, or when agencies develop or buy new IT systems to handle collections of personally identifiable information.
7. PROCEDURE. DHS published "Privacy Impact Assessments Made Simple,"(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) and this Instruction. Additionally, provide the contact information by completing enclosure (2). Send enclosures (1) and (2) to Commandant (CG-611) for review. Following DHS approval, CG-611 will submit for publication in the Federal Register.

8. ENVIRONMENTAL ASPECT AND IMPACT CONSIDERATIONS. Environmental considerations were examined in the development of this Instruction and have been determined to be 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
Acting Assistant Commandant for Command, Control,
Communications, Computers, and Information Technology

Encl: (1) Privacy Impact Assessments Made Simple
(2) Privacy Impact Assessment Contact Information



PRIVACY IMPACT ASSESSMENTS MADE SIMPLE

U.S. Department of Homeland Security
Privacy Office



INTRODUCTION: **Fundamental Principles of U.S. Privacy Protection Policy**

The Department of Homeland Security has a clear commitment to analyze and share intelligence across all of its agencies so that the urgent task of protecting the homeland can be carried out expeditiously. In this process, however, we must also have in place robust protections for the privacy of any personal information that we collect.

These protections, embodied in Federal law, seek to foster at least 3 concurrent objectives:

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

Privacy law, today, is largely a response to technological changes in computers, digitized networks, and the creation of new information products, all of which have important ramifications for the personal privacy of government records.

Recognizing these ramifications, the E-Government Act of 2002 mandates an assessment of the privacy impact of any substantially revised or new IT System. The document that accomplishes this mandate is called a Privacy Impact Assessment (PIA).



PRIVACY IMPACT ASSESSMENTS MADE SIMPLE

Technically, a Privacy Impact Assessment is an analysis of how information on individuals is handled and managed. Information on individuals can be used to identify an individual either directly – such as by name, address, social security number, email address, telephone number – or indirectly using analytical methods to derive identifiable information, thus disclosing the person’s identity. Notice the emphasis on the individual.

The E-Government Act aims to ensure that handling of this information conforms to applicable legal, regulatory, and policy requirements regarding privacy. A PIA, which answers the intent of this law, must do at least two things:

1. It must determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and
2. It must evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

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. With that in mind, to make the PIA comprehensive and meaningful, it must be a collaboration of program experts, IT experts, security experts, and privacy experts.

The length and breadth of a PIA will vary by the size and complexity of the IT project. Some projects that trigger a PIA will not be considered major and the PIA can be handled as routine. But any new systems development that has major budget implications must be able to demonstrate, through the PIA, that in-



PRIVACY IMPACT ASSESSMENTS MADE SIMPLE

depth analysis was done to ensure architectures and technologies were considered on their ability to protect privacy.

Before we discuss the details of a well constructed PIA, a brief word on how the Privacy Act of 1974 and the E-Government Act of 2002 are related would be in order.

In the case of a **new System of Records**, as defined in the Privacy Act of 1974, a PIA should be conducted while you are developing the System of Records notice (SORN). This makes sense because there are several areas that overlap in both documents such as, the categories of records in the system, the uses of the records, and the policies and practices for handling records. In addition, by developing these documents together, your office can make the PIA publicly available in the Federal Register along with the Privacy Act SORN.

In the case of **changes to an existing System of Records**, a PIA must be conducted if old legacy systems are being combined, or new data elements are being added.

We are now in a position to discuss the two fundamental components of a PIA: when to conduct a PIA, and how to conduct a PIA.

Component 1: **When to Conduct A PIA**

Not every situation requires a PIA, but it may be in the best interests of your constituency and yourself if you take the time and effort to do one, even though under the pure letter of the law you may not be obligated to do so. Remember it's about trust, and there is no better way to build trust than to put how you are going to preserve it in writing.



PRIVACY IMPACT ASSESSMENTS MADE SIMPLE

Basically the guidance is simple. Do a PIA when your office is doing **any** of the following:

- **Creating ANY new collections of personal information.** This is when you collect or pull together personally identifying information on individuals electronically that can be used to identify them particularly. One collection alone may not reveal a person's identity, but it is now technologically possible to combine data -- by using a business intelligence tool for example -- so as to reveal the true identity of some individual. In your PIA, discuss how you are going to manage these new collections and ensure they are in conformity with privacy law.
- **Developing or procuring any new technologies or systems that can store and thus reveal a person's identity.** Before any money is spent (OMB 300), your PIA should show that Privacy was considered from the beginning. It should get the same attention you give to system security and be found in your requirements and architecture documents. In fact, you should be able to reference these documents when you do your PIA to show they are on the developer's work schedule.
- **Creating new databases or views from old databases or systems.** This is very similar to the first point above, but there is a subtle difference. Changes are often made to make data access more user-friendly and effective, and often are done by special request and never get attention beyond the fix or change. Do a PIA to demonstrate that you thought about data access and Privacy when you made the changes. Remember, whenever you change things to combine data together in new



PRIVACY IMPACT ASSESSMENTS MADE SIMPLE

ways, new knowledge is likely to occur and that new knowledge may expose private information.

The intent here is obvious. If you have charge over any personal information about any individual, and you do anything that could perhaps reveal that information in any way, you must do a PIA. Now it turns out that doing a PIA is not all that tough as the next section will show.

Component 2: **How to Conduct a PIA**

Section 208 states that agencies are required to conduct PIAs for electronic information systems and collections and make them publicly available. This means that PIAs must be readable and understandable by the general public.

Questions That Must be Answered

When your systems development work creates a need to do a PIA, there are some simple steps to follow and questions to answer that will give you an easy-to-read and publishable PIA – one that will demonstrate you took the job seriously. The first step is to make sure the Privacy issues are addressed in the same manner that you address security issues.

In other words, privacy must make the overhead view-graph on your overall system architecture, just like your security requirements. Privacy must not be an afterthought. The appropriate protections must be built in before any money is spent on your new system. If you approach Privacy this way, you will have no trouble answering all of the following questions needed to do a good Privacy Impact Assessment:



PRIVACY IMPACT ASSESSMENTS MADE SIMPLE

Section 1 – Questions about the Data and its purposes:

1. What information is to be collected (e.g., nature and source)?
2. Why is the information being collected? Is it relevant and necessary to the purpose for which the system is being designed?
3. What is the intended use of the information?
4. What are the sources of the information in the system? Where and how are you acquiring the information?
5. How will the information be checked for accuracy?
6. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?
7. Will the newly derived data be placed on the individual's record?
8. Can the system make new determinations about an individual that would not be possible without the new data?
9. How will the newly derived data be verified for relevance and accuracy?
10. Are the data elements described in detail and documented? If yes, what is the name of the document?

Section 2 – Questions about redress:

1. What opportunities do individuals have to decline to provide information?



PRIVACY IMPACT ASSESSMENTS MADE SIMPLE

2. What opportunities do individuals have to consent to particular uses of the information?
3. How do individuals grant consent concerning how their information will be used or shared?
4. What are the procedures for individuals to gain access to their own information?
5. What are the procedures for correcting erroneous information?

Section 3 – Questions about access to the data:

1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others) and is it documented?
2. How will access to the data by a user be determined?
3. Are criteria, procedures, controls, and responsibilities regarding access documented?
4. Will users have role-based access to data on the system limiting them to some but not all of the data?
5. What controls are in place to prevent the misuse (e.g. browsing, expired privileges, etc.) of data by those having access?
6. Do other systems share data or have access to data in this system? If yes, explain. Include a discussion of who will be responsible for protecting the privacy rights of individuals affected by the interface?
7. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?



PRIVACY IMPACT ASSESSMENTS MADE SIMPLE

8. How will the data be used by these other agencies?
9. Who is responsible for assuring proper use of the data by other agencies?
10. How will the system ensure that other agencies only get the information they are entitled to?

Section 4 – Questions about maintenance of administrative controls:

1. Are the data secured consistent with agency requirements under the Federal Information Security Management Act? Specifically:
 - a. Affirm that the agency is following IT security requirements and procedures required by federal law and policy to ensure that information is appropriately secured;
 - b. Acknowledge that the agency has conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls;
 - c. Describe the monitoring/testing/evaluating on a regular basis to ensure that controls continue to work properly, safeguarding the information, and
 - d. Provide a point of contact for any additional questions from users.
2. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?
3. What are the retention periods of data in the system?



PRIVACY IMPACT ASSESSMENTS MADE SIMPLE

4. What are the procedures for expunging the data at the end of the retention period and are these procedures documented?
5. Will the system provide the capability to monitor individuals or groups of individuals? If yes, explain.
6. What controls are in place to prevent unauthorized monitoring of individuals or groups of individuals?
7. Under which Systems of Record Notice (SORN) does the system operate? Provide Number and Name.

Section 5 – Decision Analysis:

1. Did you evaluate competing technologies on their privacy handling capabilities? If yes, explain.
2. Were any choice changes made to system architectures, hardware, software, or implementation plans as a result of doing a PIA? If yes, explain.

Where to Go for Help

Web Site Links:

OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002: <http://www.whitehouse.gov/omb/memoranda/m03-22.html>

For a model of a PIA, the Privacy Impact Assessment for the US-VISIT Program: <http://www.dhs.gov/interweb/assetlibrary/VISITPIAfinal3.pdf>

Enclosure (1) to COMDTINST 5260.4



PRIVACY IMPACT ASSESSMENTS MADE SIMPLE

Contact us:

Privacy Office, U.S. Department of Homeland Security

Washington, DC 20528

202-772-9848

U.S. Department of Homeland Security U.S. Coast Guard CG-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 CG 611 USE ONLY

Reviewed By	Date	Approved By	Date
Comments			

Reset