National Transportation Safety Board
Privacy Impact Assessment (PIA) Procedures

Introduction

The National Transportation Safety Board is required to protect the privacy to which employees and the public are entitled by law. The Privacy Impact Assessment (PIA) provides a means for integrating the consideration of privacy issues into the development of information systems. Section I of this document provides background information on the PIA, steps for completing the PIA process, and an overview of privacy issues in information systems. Section II is the Privacy Impact Assessment tool. Section III provides a privacy impact analysis. Section IV identifies basic privacy requirements to be addressed during the systems development lifecycle.

Section I

Purpose

The Privacy Impact Assessment assists in identifying and addressing information privacy when planning, developing, implementing, and operating information systems. The PIA process gathers information for use in identifying and evaluating compliance with applicable statutory requirements. These requirements are drawn from the Privacy Act; E-Government Act as amended by the Federal Information Security Act; Government Paperwork Reduction Act; Freedom of Information Act; and Office of Management and Budget (OMB) Circulars A-130, Management of Federal Information Resources; A-123, Management Accountability; and A-11, Preparation, Submission and Execution of the Budget.

Goals accomplished in completing a PIA include the following:

- Providing senior management with the tools to make informed policy and system design or procurement decisions based on an understanding of privacy risk, and of options available for mitigating that risk;
- Ensuring accountability for privacy issues with the system project manager and system owner;
- Ensuring a consistent format and structured process for analyzing both technical and legal compliance with applicable privacy law and regulation, as well as accepted privacy policy; and
- Providing basic documentation on the flow of personal information within Safety Board systems for use and review by policy and program staff, systems analysts, and security analysts.

What is personal information?

Personal information is information about an identifiable individual that may include but is not limited to:

- Information relating to race, national or ethnic origin, religion, age, and marital or family status;
- Information relating to education, medical, psychiatric, psychological, criminal, financial, or employment history;
- Any identifying number symbol, or other particular assigned to the individual; and
- Name, address, telephone, number, finger or voice prints, or photograph.

When is a PIA required?

The Safety Board requires that PIAs be completed for all Safety Board information systems. PIAs are also required to be performed and updated as necessary when a change in a system of records creates new privacy risks. In addition, OMB requires that a PIA be submitted with Exhibit 300 for all new or significantly altered information technology investments administering information in an identifiable form collected from the public. The E-Government Act also requires publication of the PIA for websites available to the public, and websites or information systems operated by a contractor on behalf of the Safety Board for the purpose of interacting with the public.

Suppose the system I am evaluating has no personal information in it?

If the system being evaluated does not contain any personal information identifiable to an individual, complete Section II A, System Information; Section III, Privacy Impact Analysis; and Section IV, System Development Lifecycle Privacy Requirements Worksheet.

Who completes the PIA?

Since privacy must be considered when requirements are being analyzed and decisions being made about data usage and system design or procurement, the system owner and the system analyst or developer work together to complete the PIA. Once the assessment is completed, the Deputy Managing Director reviews the PIA to determine privacy risks, and the Chief Information Security Officer reviews the PIA, assesses risks, and recommends risk mitigation strategies.

When must a PIA be completed?

Privacy requirements must be identified and addressed early in the process of planning, developing/procuring, implementing, and modifying information systems that contain personal information. This requirement applies not only to Privacy Act systems of records where personal information is retrieved by the subject's name or identifier, but also any system that contains personal information.

Process for Identifying and Addressing Privacy and Security Issues

The Privacy Impact Assessment is designed to gather information necessary to identify privacy and security risks. Results of the PIA are then evaluated to identify basic privacy and security issues and requirements that are addressed during the systems development lifecycle process.

Step	Participants	Procedure
Conduct Privacy Impact Assessment		
1	System Owner and System Developer/Analyst	Obtain a copy of the PIA form and instructions. The Safety Board's Privacy Officer, Chief, Records Management Division, and the Chief Information Security Officer are available for consultation on privacy, security, records, and Freedom of Information Act issues.
2	System Owner and System Developer/Analyst	Complete the PIA.
Evaluate PIA, Identify Risks and Requirements		
3	Safety Board's Privacy Officer	Review the PIA to identify privacy risks and get clarification from the system owner and developer/analyst as needed.
4	Chief Information Security Officer	Review the PIA, assess privacy risks, identify security risks, and recommend mitigation strategies. Prepare risk assessment to document risks and mitigation strategies.
	Safety Board's Privacy Officer; Chief Information Security Officer; System Owner; System Analyst	Complete Privacy Impact Analysis.
	Safety Board's Privacy Officer; Chief Information Security Officer; System Owner; System Analyst	Complete Systems Development Privacy Requirements Worksheet
Address Privacy and Security Issues		
5	System Owner; System Developer/Analyst; Safety Board's Privacy Officer; Chief Information Security Officer	Reach agreement on design and implementation requirements to mitigate privacy and security risks.
6	System Owner and System Developer/Analyst	Incorporate the agreed upon requirements. Update the PIA to reflect elements not identified at the initial concept stage, new information collection, or choices made in designing the system or information collection as a result of the analysis

Definitions

Accuracy. Within sufficient tolerance for error to ensure the quality of the record in terms of making a determination.

Completeness. All elements necessary for making a determination are present before a determination is made.

Individual. A citizen of the United States or an alien lawfully admitted for permanent residence.

Record. Any item, collection, or grouping of information about an individual that is maintained by an agency, including but not limited to education, financial transactions, medical history, and criminal or employment history, and that contains the individual's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as finger or voice print or photograph.

Relevance. Limitation to only those elements of information that clearly bear on the determination(s) for which the records are intended.

Safety Board Information System. An information technology (IT) system that is owned, leased, or operated by the Safety Board; or that is operated by a contractor or another government agency on behalf of the Safety Board.

System of Records. A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some other personally identifying number, symbol, or other identifying particular assigned to the individual.

System Owner/Manager. Designated official responsible for this system who will ensure the implementation of legal requirements regarding information resources management (privacy, security, Freedom of Information Act, records, data administration). For a system of records, this is the system manager documented in the system of records notification.

Privacy Issues in Information Systems

- OMB Circular A-130: Management of Federal Information Resources, requires that "the individual's right to privacy must be protected in Federal Government information activities involving personal information" and that agencies will "consider the effects of their actions on the privacy rights of individuals, and ensure that appropriate legal and technical safeguards are implemented."

The Privacy Act of 1974, 5 U.S.C. 552a, requires federal agencies to protect personally identifiable information. For example, it states the following specifically:

> Each Agency that maintains a system of records shall—
>
> - maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President;
> - collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's right's benefits, and privileges under Federal programs;

- inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual-" of the authority which authorizes the solicitation of the information and whether disclosure of the information is mandatory or voluntary, principle purpose and routine uses of the information being collected from them, and any effects upon the individual of not providing all or part of the requested information;
- maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination;
- establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and requirements of this section, including any other rules and procedures adopted pursuant to this section and the penalties for noncompliance;
- establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to the individual on whom the information is maintained.

OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, dated September 26, 2002, states the following:

> Agencies must consider the information lifecycle (i.e. collection, use, retention, processing, disclosure and destruction) in evaluating how information handling practices at each stage may affect individual's privacy. To be comprehensive and meaningful, privacy impact assessments require collaboration by program experts as well as experts in the areas of information technology, IT security, records management, and privacy.

OMB Memorandum M-99-05, Instructions on Complying with President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records," dated January 7, 1999, states the following:

> Systems of records should not be inappropriately combined. Groups of records which have different purposes, routine uses, or security requirements, or which are regularly accessed by different members of the agency staff, should be maintained and managed as separate systems of records to avoid lapses in security. Therefore, agencies shall ensure that their system of records do not inappropriately combine groups of records which should be segregated. This ensures, for example, that routine uses which are appropriate for a certain group of records do not also apply to other groups of records simply because they have been placed together in a common system of records.

Section II

Safety Board Privacy Impact Assessment

A. System Information
1. What is the system name? **Docket Management System (DMS)**
2. What is the purpose and intended use of this system? **The NTSB uses this public facing web based system to provide relevant information related to accident investigations to the general public.**
3. Does this system contain any personal information about individuals? (If no, a PIA is not required. Skip to Section III.) Yes.
4. What legal authority authorizes the purchase or development of this system/application? (List the statutory provisions or Executive Orders that authorize the maintenance of this information to meet an official program mission or goal.) **Title 49 of the United States Code, Chapter 11.**
5. For new systems, describe how privacy is addressed in documentation related to system development, including as warranted and appropriate, statement of need, functional requirements analysis, alternatives analysis, feasibility analysis, benefits/cost analysis, and especially, the initial risk assessment. **The Docket Management System is not a new system, posting of dockets to the web is part of the NTSB's overall FOIA improvement Plan in response to Executive Order 13,392.**

B. Data in the System
1. What categories of individuals are covered in the system (for example, employee, contractor, public)? **The public, employees of modal transportation carriers, employees of equipment manufacturers, experts in relevant disciplines and public officials involved with the investigative process.**
2. What are the sources of information in the system? **NTSB investigators and individuals.** **a. Is the information collected directly from the individual or is it taken from another source? If information is not collected directly from the individual, describe the source of the information.** **When possible the information is collected directly from the individual. In some**

instances the data may be obtained from other sources, to include carrier records.

b. What federal agencies provide data for use in the system?
None.

c. What state and local agencies provide data for use in the system
None.

d. What other third parties will data be collected from?
Transportation providers, manufacturers, parts and maintenance suppliers, government regulatory agencies, experts and other parties involved in the investigation.

e. What information will be collected from the employee and the public? (Be as specific as possible. List personal information collected from the public such as Social Security Number, address, credit card number, telephone number. Employee information may include badge number, user identifier, telephone number, social security number, and health information.)
Information relevant to support the investigation of the incident/accident and to determine probable cause will be collected and entered into the Docket Management System (DMS). However, information presented in the web based DMS system will have passed several quality control steps designed to ensure the redaction of PII data not already in the public domain.

3. How does the Safety Board ensure that data are sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations about any individual?

a. How is data accuracy ensured?
The data is reviewed by multiple individuals with the originating modal office as part of a standard quality review process.

b. How will data be checked for completeness?
The data is checked for completeness as part of the overall investigation process and as part of the standard quality review process.

c. Are the data current? What steps or procedures are taken to ensure the data are not out of date?
Data contained in the DMS system is current. In the event that corrections or updates are required, changes will be included and an errata sheet will be placed in the docket to highlight corrections.

d. Are the data elements described in detail and documented? If yes, what is the name of the document?

Data elements are not described in detail. The web based Docket Management System is a collection of documents relevant to a specific incident or accident and are primarily textual in nature. Component parts such as charts, pictures, etc., are adequately described in the context of each docket entry.

e. How will data collected from sources other than NTSB records be verified for accuracy?

Data is verified through various means to include: review of public data, verification with original parties and sources, and through a structured fact-finding investigative process. Internal quality control processes are also in place to ensure completeness and accuracy of data present in the system prior to posting to the NTSB's public web site.

4. Describe what opportunities individuals have to decline to provide information (that is, where providing information is voluntary) or to consent to particular uses of information (other than required or authorized uses), and how individuals can grant consent.)

Congress has specifically directed the Safety Board to collect information that the Board organizes in its Docket Management System (DMS). In instances in which a person requests that the Safety Board refrain from making certain information publicly available through the DMS public interface, the Board will consider such requests in accordance with its regulations, at 49 C.F.R. § 831.6(b), which allow for the Board to consider whether the public interest in disclosure outweighs the requester's objection.

C. Attributes of the Data

1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

Yes.

2. Will the system derive new data or create previously unavailable data about an individual through the aggregation of information collected? (If no, skip to C.3.)

No.

a. Will the new data be placed in the individual's record?

f. **Can the system make determinations about employees or the public that would not be possible without the new data?**

c. **How will the new data be verified for relevance and accuracy?**

3. Do the records in this system share the same purpose, routine use, and security requirements?

Yes.

a. **If the data are being consolidated, what technical, management, and operational controls are in place to protect the data from unauthorized access or use? Explain.**

b. **If processes are being consolidated, are the proper technical, management, and operational controls remaining in place to protect the data and prevent unauthorized access? Explain.**

4. How will the data be retrieved? Can a personal identifier be used to retrieve data? Are personal identifiers used to retrieve data on a routine, occasional, or ad hoc basis? If yes, explain and list the identifiers what will be used to retrieve information on the individual.

No.

5. What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

Reports can be generated for administrative purposes on investigations done each NTSB investigator.

D. Maintenance of Administrative Controls
1. If the system is hosted and/or used at more than one site, how will consistent use of the system and data be maintained at all sites? **The system is hosted at one site.**
2. What are the retention periods of the data in this system? **The DMS system is intended to be a historical record of accidents investigated by the Safety Board. As such, the NTSB will maintain records in DMS for the foreseeable future.**
3. What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented? **Not applicable at this time.**
4. Is the system using technologies in ways that the Safety Board has not previously employed (for example, monitoring software, CallerID)? If yes, how does the use of this technology affect public/employee privacy? **No.**
5. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain. **No.** **a. What kinds of information are collected as a function of the monitoring of individuals?** **b. What controls will be used to prevent unauthorized monitoring?**
6. Under which Privacy Act systems of records notice does the system operate? Provide name and number. **The Safety Board's use of the Docket Management System (DMS) does not require a System of Records Notice under the Privacy Act, because DMS does not meet the definition**

of a "system of records." 5 U.S.C. § 552a(a)(5) (defining a system of records as "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual"). Information in DMS is not retrievable by individuals' names or other unique identifiers. Therefore, no system of records notice exists for DMS.

7. If the system is being modified, will the Privacy Act system of records notice require amendment of revision? Explain.

Not applicable.

E. Access to Data

1. Who will have access to the data in the system (for example, contractors, users, managers, system administrators, developers, other)?

Data in the system is available to the general public via the entry of search criteria entered into the Safety Board's public website.

2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

Access to data is granted to the public via NTSB's internet site at www.ntsb.gov

3. Will users have access to all data on the system or will the user's access be restricted? Explain.

The public has access to a subset of data that is part of the public record. Access to data is restricted by the use of a physically separate database which is made available on the public interface. Information used to populate the public database is reviewed as part of the standard quality control process which prohibits access to non-public data and information.

4. What controls are in place to prevent the misuse (for example, unauthorized browsing) of data by those having access? List procedures and training materials.

The public interface only allows access to publicly available data and information.

5. Are contractors involved with the design and development of the system and/or will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?

Yes. Appropriate non-disclosure agreements are part of the contract.

6. Do other systems share data or have access to the data in the system? If yes, explain. **Data stored in the Docket Management System (DMS) is a compendium of information available to the Safety Board for a particular incident or accident. Data contained in DMS may also exist in other forms in various systems at the Safety Board.**
7. Who will be responsible for protecting the privacy rights of the public and employees affected by the interface? **The information present in the web based Docket Management System is publicly available information. Privacy rights are protected by not allowing display of PII data that is not already in the public domain. The privacy rights of the public and employees are protected by the Safety Board's Senior Agency Official for Privacy and Privacy Officer as well as by policies and procedures related to the protection of PII data.**
8. Will other agencies share or have access to the data in this system? If yes, list agencies. **The information is available to the public and per policy the Safety Board does not employ permanent cookies to track site access. It is not possible to provide a list of customers by individual or organization to the web based Docket Management System.**
9. How will the data be used by the other agency? **The Safety Board does not track how the publicly available information is used.**
10. Who is responsible for ensuring proper use of the data? **See response to questions 8 & 9.**

Section III

Privacy Impact Analysis

System of Records Identification
1. Is a system of records being created under the Privacy Act, 5 U.S.C. 552a? If no, skip questions 2 through 4. **No.**
2. Have privacy and IT risk assessments been conducted that consider the alternatives to collection and handling as designed and the appropriate measures to mitigate risks identified for each alternative?
3. What impact will this system have on an individual's privacy? (Consider the consequences of collection and flow of information and identify and evaluate threats to individual privacy.)
4. As a result of the PIA, what choices have been made regarding the IT system of collection of information? Have adequate measures been designed and implemented to mitigate risk? What is the rationale for the final design choice or business process?

Section IV

System Development Lifecycle Privacy Requirements Worksheet

A. Contact Information
1. Person who completed the Privacy Impact Assessment document Name: **Melba D. Moye** Title: **Chief, Records Management Division** Organization: **NTSB/Office of the Chief Information Officer** Phone number: **202-314-6551**
2. System Owner Name: **Melba D. Moye** Title: **Chief, Records Management Division** Phone number: **202-314-6551**
3. IT Security Reviewer Name: **Chris Stephens** Title: **Chief Information Security Officer** Organization: **NTSB/Office of the Chief Information Officer** Phone number: **202-314-6599**
4. Safety Board Privacy Reviewer Name: **David Mayer** Title: **Deputy Managing Director and Senior Agency Official for Privacy** Organization: **NTSB/Office of the Managing Director** Phone number: **202-314-6318**

Privacy Impact Assessment Summary		
CB	**System Category**	**Requirement**
☐	System of Records	Publish System of Records Notice
☒	Website available to the public	Publish Privacy Impact Assessment
☐	Website or information system operated by a contractor on behalf of the Safety Board for the purpose of interacting with the public	Publish Privacy Impact Assessment
☐	New or significantly altered information technology investment administering information in an identifiable form collected	Conduct Privacy Impact Assessment

	from or about members of the public	
☐	New or significantly altered information technology investment administering information in an identifiable form collected from or about Safety Board employees	Conduct Privacy Impact Assessment
☐	Contains medical information	Determine if system is subject to HIPAA
☐	Other	
☐	None of the above	Privacy Impact Assessment not required

Privacy Impact Assessment Approval
Approval of Privacy Impact Assessment accuracy and completeness. **System Owner:** [redacted] (Signature) 6/25/09 (Date) Name: **Melba D. Moye** Title: **Chief, Records Management Division**
Approval of IT System Risk Assessment **Chief Information Security Officer:** [redacted] (Signature) 6/25/09 (Date) Name: **Chris Stephens** Title: **Chief Information Security Officer**
Approval of Privacy Assessment and Resulting System Category **Senior Privacy Officer:** [redacted] (Signature) 6/25/2009 (Date) Name: **David Mayer** Title: **Deputy Managing Director and Senior Agency Official for Privacy**