

**U.S. International Boundary & Water Commission (USIBWC)
Information Management Division (IMD)**



Privacy Impact Assessment (PIA)

**For the
Legal Affairs Office**

Date: January 13, 2017

CONTACT INFORMATION AND BACKGROUND

Date Submitted to IMD: January 13, 2017		PIA Status <input checked="" type="checkbox"/> New <input type="checkbox"/> Updated	Agency: U.S. International Boundary & Water Commission (USIBWC)
System/Project Name: General Support System/ Legal Affairs Office		System/Project Acronym: GSS/Legal Affairs Office	
Sponsoring USIBWC Division or Office: IMD			
Person Completing this PIA Form		Information Security Manager for this System/Project	
Name: Hector A. Villalobos Title: IT Specialist / Information Systems Security Officer Division: IMD Telephone: 915-832-4708		Name: Zenon Mora Title: Supervisory, IT Specialist / ISSM Division: IMD Telephone: 915-832-4755	
System Owner for this System/Project		Program Manager for this System/Project	
Name: Maritza Dominguez Title: IT Specialist / Network Administrator Division: IMD Telephone: 915-832-4130		Name: Matthew Myers Title: Chief Legal Counsel Division: Legal Affairs Office Telephone: 915-832-4728	
Privacy Office or Designee		Reviewing Official	
Name: Matthew Myers Title: Chief Legal Counsel/Senior Agency Official on Privacy Division: Legal Affairs Office Telephone: 915-832-4728		Name: Diana Forti Title: Chief Information Officer (CIO) Division: Administrative Department Telephone: 915-832-4123	
Additional Points of Contact (POCs) / Subject Matter Experts for this System/Project (if applicable)			
POC's Name: Title: Division: Telephone Number:		POC's Name: Title: Division: Telephone Number:	
POC's Name: Title: Division: Telephone Number:		POC's Name: Title: Division: Telephone Number:	

Section 1.0: Introduction

In accordance with federal regulations and mandates¹, the USIBWC conducts Privacy Impact Assessments (PIAs) on systems, business processes, projects and rulemakings that involve an *electronic* collection, creation, maintenance or distribution of personally identifiable information (PII).² The objective of a Privacy Impact Assessment is to identify privacy risks and integrate privacy protections throughout the development life cycle of an information system or electronic collection of PII. A completed PIA also serves as a vehicle for building transparency and public trust in government operations by providing public notice to individuals regarding the collection, use and protection of their personal data.

To fulfill the commitment of the USIBWC to protect personal data, the following requirements must be met:

- Use of the information must be controlled.
- Information may be used only for necessary and lawful purposes.
- Information collected for a particular purpose must not be used for another purpose without the data subject's consent unless such other uses are specifically authorized or mandated by law.
- Information collected must be sufficiently accurate, relevant, timely, and complete to ensure the individual's privacy rights.

Given the vast amounts of stored information and the expanded capabilities of information systems to process the information, it is foreseeable that there will be increased requests, from both inside and outside the USIBWC, to share sensitive personal information.

Upon completion of this questionnaire and prior to acquiring signatures, please email the form to the ISSM /ISSO: z.mora@ibwc.gov & hector.villalobos@ibwc.gov who will review your document, contact you with any questions, and notify you when the PIA is ready to be routed for signatures.

Section 2.0: System/Project Description

2.1 In this section of the Privacy Impact Assessment (PIA), describe the system/project and the method used to collect, process, and store information. Additionally, include information about the business functions the system/project supports.

The Legal Affairs Office (LAO) receives some information with PII if the information is part of a case that is being litigated in a federal court, board or commission. The LAO also receives information with PII as part of a request for a legal review. All information is secured behind locked doors.

Section 3.0: Data in the System/Project

The following questions address the type of data being collected and from whom (nature and source), why the data is being collected (purpose), the intended use of the data, and what opportunities individuals have to decline to provide information or to consent to particular uses of their information.

3.1 What personally identifiable information (PII) (e.g., name, social security number, date of birth, address, driver's license, passport, financial account, etc.) will be collected, used or maintained in the system? Explain.

The LAO does not collect any specific PII. Sometimes requests for legal review and cases in litigation include identifying PII.

¹ [Section 208 of the E-Government Act of 2002](#) requires federal government agencies to conduct a Privacy Impact Assessment (PIA) for all new or substantially changed technology that collects, maintains, or disseminates personally identifiable information (PII). Office of Management and Budget (OMB) Memorandum [M-03-22](#) provides specific guidance on how Section 208 should be implemented within government agencies. The [Privacy Act of 1974](#) imposes various requirements on federal agencies whenever they collect, create, maintain, and distribute records that can be retrieved by the name of an individual or other personal identifier, regardless of whether the records are in hardcopy or electronic format. Additionally, [Section 522](#) of the 2005 Consolidated Appropriations Act requires certain Federal agencies to ensure that the use of technology sustains, and does not erode, privacy protections, and extends the PIA requirement to the rulemakings process.

² For additional guidance about USIBWC rulemaking PIAs, contact the IMD ISSM / ISSO Staff at (z.mora@ibwc.gov & hector.villalobos@ibwc.gov).

3.2 What is the purpose and intended use of the information you described above in Question 3.1? (e.g., For administrative matters, For criminal law enforcement activities, To conduct analysis concerning subjects of investigative For litigation or other interest, etc.)

The PII in documents sent to the LAO are for identification of parties or for litigation.

3.3 Who/what are the sources of the information in the system? How are they derived? (e.g., In person, telephone, email, hard copy, online, etc.)

The sources of the information are USIBWC supervisors, managers and Executives who provide the information in person or by e-mail.

3.4 What Federal, state, and/or local agencies are providing data for use in the system? What is the purpose for providing data and how is it used? Explain.

The LAO does not usually receive PII from state or local agencies. Sometimes we receive a claim from an accident by a USIBWC employee and the state or local agency seeks reimbursement for damages caused by the USIBWC employee.

3.5 What other third-party sources will be providing data to the system? Explain the data that will be provided, the purpose for it, and how will it be used.

No other third party sources provided data to the system.

3.6 Do individuals have the opportunity to decline to provide personal information and/or consent only to a particular use of their data (e.g., allowing basic use of their personal information, but not sharing with other government agencies)?

Yes Explain the issues and circumstances of being able to opt out (either for specific data elements or specific uses of the data):

Individuals who do not provide information that is necessary for them to process their case may not be allowed by a forum to continue with their litigation.

No Explain:

Section 4.0: Data Access and Sharing

The following questions address who has access to the data, with whom the data will be shared, and the procedures and criteria for determining what data can be shared with other parties and systems.

4.1 Who will have access to the data in the system (internal and external parties)? Explain their purpose for having access to this information.

Court, board or Commission personnel may have access to limited, identifying PII.

4.2 How is access to the data determined and by whom? Explain the criteria, procedures, controls, and responsibilities for granting access.

The presiding judge of the relevant court, board or commission determines who has access.

4.3 Do other systems (internal or external) receive data or have access to the data in the system? If yes, explain.

No

Yes Explain.

4.4 If other agencies or entities use data in the system, explain the purpose for sharing the data and what other policies, procedures, controls, and/or sharing agreements are in place for protecting the shared data.

N/A

4.5 Who is responsible for assuring proper use of data in the system and, if applicable, for determining what data can be shared with other parties and systems? Have policies and procedures been established for this responsibility and accountability? Explain.

The attorneys of record and the judges of the relevant courts, boards and commissions.

4.6 What involvement will a contractor have with the design and maintenance of the system? Has a Contractor Confidentiality Agreement or a Non-Disclosure Agreement been developed for contractors who work on the system?

None.

Section 5.0: Data Integrity and Security

The following questions address how data security and integrity will be ensured for the system/project.

5.1 How is data in the system verified for accuracy, timeliness, and completeness?

Information is compared to other information in HR and is verified by the forum that has the litigation.

5.2 What administrative and technical controls are in place to protect the data from unauthorized access and misuse? Explain.

Information is maintained in locked offices, locked filing cabinets, and in computer drives with limited access (only by LAO personnel).

Section 6.0: Data Maintenance and Retention

The following questions address the maintenance and retention of records, the creation of reports on individuals, and whether a system of records is being created under the Privacy Act, 5 U.S.C. 522a.

6.1 How is data retrieved in the system or as part of the project? Can it be retrieved by a personal identifier, such as name, social security number, etc.? If yes, explain, and list the identifiers that will be used to retrieve information on the individual.

Physical files are retrieved by names. Electronic files are filed with names or other legal identification (such as *Party Vs.* USIBWC)

6.2 What kind of reports can be produced on individuals? What is the purpose of these reports, and who will have access to them? How long will the reports be maintained, and how will they be disposed of?

Case status reports can be produced for LAO personnel to monitor and track the case in litigation. Upon closure of the case file, the file is destroyed in accordance with NARA regulations.

6.3 What are the retention periods of data in this system? What are the procedures for disposition of the data at the end of the retention period? Under what guidelines are the retention and disposition procedures determined? Explain.

Legal disposition and retention periods follow IBWC Records Management and NARA regulations.

6.4 In the Federal Register, under which Privacy Act Systems of Record Notice (SORN) does this system operate? Provide number and name.

N/A

6.5 If the system is being modified, will the Privacy Act SORN require amendment or revision? Explain.

N/A

Section 7.0: Business Processes and Technology

The following questions address the magnitude of harm if the system/project data is inadvertently disclosed, as well as the choices the agency made regarding business processes and technology.

7.1 Will the system aggregate or consolidate data in order to make privacy determinations or derive new data about individuals? If so, what controls are in place to protect the newly derived data from unauthorized access or use?

No.

7.2 Is the system/project using new technologies, such as monitoring software, SmartCards, Caller-ID, biometric collection devices, personal identification verification (PIV) cards, radio frequency identification devices (RFID), virtual data rooms (VDRs), social media, etc., to collect, maintain, or track information about individuals? If so, explain how the use of this technology may affect privacy.

No.

7.3 Will the system/project provide the capability to monitor individuals or users? If yes, describe the data being collected. Additionally, describe the business need for the monitoring and explain how the information is protected.

No.

7.4 Explain the magnitude of harm to the agency if privacy-related data in the system/project is disclosed, intentionally or unintentionally. Would the reputation of the agency be affected?

Unauthorized release may cause great harm. The reputation of the agency would be affected.

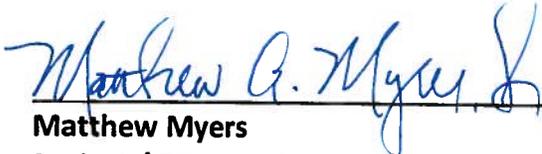
7.5 Did the completion of this PIA result in changes to business processes or technology? If yes, explain.

Yes. The IMD will provide the recommendations from section 2.1 to Executive Management of the USIBWC. Any approved recommendations will be converted into action items and tracked by the SOAP and the IMD. PIA assessments are a good reminder to identify privacy risks and integrate privacy protections and mitigate vulnerabilities.

Privacy Impact Assessment Authorization Memorandum

(Note: Do not route this form for signature until you have received approval from the IMD Staff.)

This system or application was assessed and its Privacy Impact Assessment approved for publication.



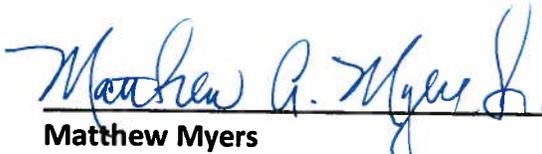
Matthew Myers
Project / Program Manager

Feb. 16, 2017
Date



Zenon Mora
Information Security Manager

MARCH 17, 2017
Date



Matthew Myers
Privacy Office or Designee

Feb. 16, 2017
Date



Diana Forti
Reviewing Official

5/9/17
Date