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

INTERNATIONAL BOUNDARY AND WATER COMMISSION
COMISION INTERNACIONAL DE LIMITES Y AGUAS

Privacy Impact Assessment (PIA)

For the

Public Affairs & Foreign Affairs Office

Date: January 13, 2017

CONTACT INFORMATION AND BACKGROUND

Date Submitted to IMD: January 13, 2017	**PIA Status** □ New ☒ Updated	**Agency: U.S. International Boundary & Water Commission (USIBWC)**

System/Project Name: General Support System / Public Affairs Office	**System/Project Acronym: GSS / PAO**

Sponsoring USIBWC Division or Office: IMD

Person Completing this PIA Form Name: Hector A. Villalobos Title: IT Specialist / Information Systems Security Officer Division: IMD Telephone: 915-832-4708	**Information Security Manager for this System/Project** Name: Zenon Mora Title: Supervisory, IT Specialist / ISSM Division: IMD Telephone: 915-832-4755
System Owner for this System/Project Name: Maritza Dominguez Title: IT Specialist / Network Administrator Division: IMD Telephone: 915-832-4130	**Program Manager for this System/Project** Name: Sally Spener Title: Foreign Affairs Officer / Public Affairs Officer Division: Public Affairs Office Telephone: 915-832-4175
Privacy Office or Designee Name: Matthew Myers Title: Chief Legal Counsel/ Senior Agency Official for Privacy Division: Legal Affairs Office Telephone: 915-832-4728	**Reviewing Official** 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 mandates[1], 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.

An Access database exists with contact information for hundreds of stake holders, Congressmen, State, Local and Federal Points of Contact, Citizen's Forum members (past and present). Information is entered into the database by PAO or FAO staff. It is entered into the personal GroupWise address book for the PAO and USIBWC Secretary's use by USIBWC staff. Information is used to contact individuals by telephone, mail, or email about Commission activities, meetings, and events. Business cards and other limited contact information are also stored in a hard copy Rolodex. The database is used to store and maintain contact information, create mailing labels, properly address envelopes, and letters.

Section 3.0: Data in the System/Project

[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).

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.

Name, address, phone number, fax number, email. Passport for USIBWC staff with official/government passports and for others who are participating in IBWC-sponsored meetings in Mexico. Information collected is available on business cards provided by the stakeholder or employee.

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.)

To communicate with the individuals about USIBWC projects, activities, and events. To facilitate crossing of personnel across the international boundary.

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.)

Sources include sign-in sheets from meetings, business cards provided by the individuals, Citizens Forum application forms completed by individuals, emails received from individuals, information provided on the telephone or in person, publicly-available information such as online listings of city council members. Passport info is provided by the bearers.

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.

No data received from these entities is provided to other agencies or systems. Only contact information for individuals who are employed by local, state, or federal government.

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.

N/A

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):

Citizens Forum application explains that people may opt out of providing information.

☐ 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.

Public Affairs staff have access to the database to perform data entry, updates or to send mass mailings, emails, or make phone calls to the individuals about Commission business. Contact information of certain individuals may be provided to other USIBWC offices if they have a need to conduct official business with the contacts (such as mailing Citizens Forum meeting notices). Citizens Forum board rosters provided to USIBWC contractor for purposes of contacting board members about Citizens Forum meetings.

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

Determined by the IMD (who controls access to the network drive where the database resides) and by the Public Affairs staff. GroupWise address books are not available unless the address book is shared with a USIBWC staff member by the Foreign Affairs Officer. Mailing labels are compiled by Public Affairs staff and emailed to USIBWC field offices for purposes of mailing out Citizens Forum meeting notices. Information is not available nor searchable in an agency-wide or public database. Periodic training provided to staff in proper use of PII.

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.

See reply to 4.2 above. PII policies prohibit sharing of PII to outside entities or others who do not have a need to know. Over the years, Public Affairs Office has received various requests from outside entities for a copy of our mailing list for activities other than Commission business. Public Affairs Officer reviewed these requests and denied them as being inconsistent with PII guidelines.

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?

N/A

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?

When mail is returned or emails bounce back, the information is updated. When new sign-in sheets come are collected, the database is updated. After elections, contact information for office holders is updated. All of the above is subject to availability of staff to perform these functions.

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

Agency has procedures that limit access to computer systems to authorized users for authorized purposes (such as PIV cards, passwords, restricted access to network drives, etc.). A password has been applied to the database to restrict access

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.

In GroupWise address book, information can be retrieved by name, employer/affiliation, and email address.
In Access database, all fields can be searched or sorted. The most common use is to search by mailing list so that a set of mailing labels is produced for all individuals who are coded as being part of a certain mailing list (like Colorado River Citizens Forum mailing list). If we need to place a telephone call to an individual or update an individual's mailing address, we can search that individual's name. Database fields consist of: ID, Display Name, email address, first name, middle name, last name, street, city, state/province, zip/postal code, country, business phone, business fax, job title, organization, department, greeting business comments, mailstop, Location, Term Exp, Mailing List, CF Board, Last Update, Newsletter Mailing, Mailing list.

By having multiple fields, we can limit the lists we compile from the database to only certain individuals or types who are appropriate to contact for a given purpose.

Not all fields are used for all individuals.

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?

No reports produced for individuals. For individuals, we only compile mailing/distribution lists if we have need to contact a group of individuals for a given project, activity, meeting, or event.

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.

FAO and PAO 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.

In order to access the system where the database is stored, a user must have a PIV card to access the PC and be granted access to the EXE shared drive.

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.

IMD has the ability to monitor USIBWC staff use of computers where database information is entered/stored.

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?

The vast majority of sensitive information in the Citizens Forum database is already available publicly, such as through the telephone book or online. Private entities routinely sell and share the type of information in the USIBWC database for marketing purposes. It is doubtful any of the individuals would even notice if there was an increase of telemarketing or direct mail marketing or spam as a result of disclosure of the information held by USIBWC.

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

Good reminder about PII. 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.

Additional Notes:

During this Assessment, FAO and PAO was found to maintain digital files containing sensitive and PII information in the following locations:

- The Access database located (Actual Server Location, 192.168.45.29): G:\DATA4\GROUPS\EXE\PAO DATABASE
- Foreign Affairs Passport/ IBWC ID Card Applications:
Data (Actual Server Location, 192.168.45.29): G:\DATA4\GROUPS\EXE\Foreign Affairs Office
- IBWC ID Application stored on Endpoint Name: HQ-EXE-IDCARD (Contains Company, Location/Type of Work, Name, Title, Nationality, Place of Birth, Date of Birth, Height, Hair Color, Eye Color, Identification Marks and Signature) This workstation has no internet or GSS connectivity, it is a stand alone system.

Recommended Actions	Status
FAO and PAO should ensure all staff are aware of process when receiving PII from other departments or agencies. Assessments have detected that FAO and PAO receives SBU and PII either physically or electronically, but information is not always encrypted. Security staff should ensure that any SBU or PII received is protected with encryption (WinZip), password protected files or redaction.	FAO and PAO has developed internal process to address this recommended action. Employees have been made are aware of the special handling and sensitivity of the information they collect and take the appropriate steps to safeguard it.
Verify HQ shredding contract complies with Federal regulations when shredding PII. Documents containing PII with expired retention periods should be destroy.	PII that is placed in established shred bins throughout HQ meet the federal regulation requirements for shredding PII.
FAO and PAO staff should follow established IBWC policies when dealing with PII.	The IT Access Control Policy and IBWC Handbook on the proper handling of PII can be used to train and provide guidance to anyone found to not follow established guidance on the proper handling of PII.
Recommend modifying permissions to only allow FAO and PAO to access PII and not the entire Executive group.	The IMD has applied a password on the database to ensure only FAO/PAO personnel can access the database.
FAO and PAO stores hard copy documents with PII in locked cabinets. An assessment should be conducted to determine if these hard copies are necessary to be kept since electronic versions should already exist. All file cabinets and folders should be identified/labeled as Sensitive But Unclassified (SBU).	The IBWC internal auditor or FAO and PAO staff should conduct this assessment and help improve existing business practices. A "SBU" stamp can be ordered from RMO to ensure all documentation is property identified.
FAO and PAO staff should receive records management (retention/disposition) training and internal policies and procedures be updated.	Recommend scheduling training with RMO staff.
Training of all FAO and PAO staff on how to encrypt files/folders using WinZip, Adobe, Office products so sensitive information can be sent securely over email.	One on one training has been provided to FAO and PAO staff as necessary on access and protection of the information within the database. The IBWC Handbook on PII protection also provides guidelines and training.
The IMD create an encrypted shared server space restricted only to SBU documentation for secure storage.	The IMD will be implementing network encryption capabilities where all PII will be securely stored. This should be in place by the end of the second quarter of 2017.

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.

2/28/17

Sally Spener
Project / Program Manager

Date

Digitally signed by MANUEL MORA
DN: c=US, o=U.S. Government, ou=Department of State, ou=U.S. and Mexico International Boundary and Water Commission, cn=MANUEL MORA, 0.9.2342.19200300.100.1.1=19001000345821
Date: 2017.03.19 09:46:24 -06'00'

Zenon Mora
Information Security Manager

Date

Matthew Myers
Senior Agency Official for Privacy

Date

3/9/17

Diana Forti
Reviewing Official

Date