

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



Privacy Impact Assessment (PIA)

For the

Equal Employment Opportunity (EEO)

Date: January 13, 2017

CONTACT INFORMATION AND BACKGROUND

Date Submitted to IMD: January 13, 2017		PIA Status <input type="checkbox"/> New <input checked="" type="checkbox"/> Updated	Agency: U.S. International Boundary & Water Commission (USIBWC)
System/Project Name: General Support System / Equal Employment Opportunity		System/Project Acronym: GSS / EEO	
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: Frances Castro Title: Equal Employment Opportunity Officer Division: Equal Employment Opportunity Office Telephone: 915-832-4112	
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 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.

Some PII or Sensitive information is provided by employees, applicants for employment in the USIBWC and sometimes contractors filing complaints against the USIBWC. The documents are used to support their allegations of discrimination. Sometimes the Agency will provide information to support the agency's position on the complaints. Both electronic and physical files are filed and maintained as mandated by the EEOC Management Directive 110. Originals, un-redacted are kept in the EEO office, and the office and files are kept locked when no one is in the office. Only redacted copies of files and documents are sent to EEOC, attorneys, representatives, etc, as needed.

Information will be used (a) as a data source for complaint information for production of summary descriptive statistics and analytical studies of complaints processing and resolution efforts (b) to respond to general requests for information under the Freedom of Information Act; (c) to respond to requests from legitimate outside individuals or agencies (White House, Congress, Equal Employment Opportunity Commission) regarding the status of an EEO complaint or appeal; or (d) to adjudicate complaint or appeal.

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 rulemaking process.

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

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 EEO Office collects names, Date of Birth, addresses and in some cases financial and personnel information. EEO should not place non-relevant information in complaint files. Where names, social security numbers, home addresses, and any other personal identifying information are not relevant, that information is redacted before the document containing them is included in the complaint file. Relevant information that should not be redacted includes management and/or comparative employees'/applicants' names. Once a document is included in the complaint file, the complainant has a right to the entire file. All parties including the agency representative, the complainant and his/her counsel, and the Administrative Judge should all have the same complaint file, either without redactions or containing the same redactions.

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 purpose of the collection and retention of this information is for EEO investigations, EEOC hearings and litigations in EEO complaint cases.

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 information are the Complainant, the Agency, HR, management and the attorneys. The information is usually derived either in person, hard copy or via 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.

None. The information received for EEO investigations comes from management, the Complainant or the Human Resources office.

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):

No Explain: The information is required as part of the case.

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.

All parties including the agency representative, the complainant and his/her counsel, and the Administrative Judge should all have the same complaint file, either without redactions or containing the same redactions

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

Access is determined by the Agency EEO Officer. The EEO Officer follows Management Directive 110 (MD-110) in determining who gets a copy of the redacted information.

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. Contract counselors, investigators and mediators will have access to redacted information, unless the information is submitted by the complainant to them. Contractors are responsible for redacting PII if they receive information from the Complainant. The EEO Office is responsible for redacting PII information prior to sending it to Complainant, Complainant's attorney/representative, Agency and the EEOC.

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.

No other agencies. Information is submitted after being redacted. PII is removed before sharing it with EEOC and attorneys.

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 EEO Officer and the legal office are responsible for assuring proper use of data and determining what data can be share. Data that is part of an EEO investigation is reviewed by the legal office prior to it being given to a contract investigator.

The EEO Officer has no control over data submitted by complainants to the EEO office or directly to investigators, attorneys, EEO counselors and EEOC judge.

The EEO Officer developed IBWC Form 258 and inserted Privacy Act Statement on her EEO forms:

PRIVACY ACT STATEMENT (5 U.S.C. §552a) AUTHORITY:

PRINCIPAL PURPOSE: Used for processing of complaints of discrimination because of race, color, religion, sex, national origin, age, physical or mental disability, genetic information, and/or reprisal by USIBWC civilian employees, former employees, and applicants for employment.

ROUTINE USES: Information will be used (a) as a data source for complaint information for production of summary descriptive statistics and analytical studies of complaints processing and resolution efforts (b) to respond to general requests for information under the Freedom of Information Act; (c) to respond to requests from legitimate outside individuals or agencies (White House, Congress, Equal Employment Opportunity Commission) regarding the status of an EEO complaint or appeal; or (d) to adjudicate complaint or appeal.

DISCLOSURE: Voluntary, however, failure to complete all appropriate portions of the form may lead to delay in processing and/or rejection of complaint on the basis of inadequate data on which to continue processing.

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?

A contractor has no involvement in the design and maintenance of the system. Contractor confidentiality agreement or non-disclosure agreement have not been developed. Data given to contractors by the EEO office has been redacted prior to being given for their use. The EEO Office has no control over data submitted by complainants directly to contract investigators, contract mediators or contract EEO counselors.

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?

EEO cases are legal cases and the data that is submitted is done so to support allegations of discrimination. The EEO office is not the entity in charge of verifying data for accuracy, timeliness and completeness.

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

The EEO Office has internal controls in place to protect the data from unauthorized access and misuse. Complaints files and inside the EEO Office, and they office is kept locked when no one is in the office.

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.

The EEO Office assigns case numbers to all cases. Cases are filed and data can be retrieved by looking for the case number or the complainant's name. Example of a case number is USIBWC EEO010116. No PII data is available in the case numbers.

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?

Number of complaints and basis of the complaints. Reports are maintained 5 years after the cases are closed. After that a memorandum is sent to the legal office letting them know that the cases will be destroy. Cases are shredded or taken to the shredding box for a contractor to shred them.

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.

EEO 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?

Highly sensitive information is kept on the IBWC GSS network. The USIBWC reputation would be greatly effected in a negative way if data was disclosed intentionally or unintentionally.

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

Yes, Additional internal SOP's will be developed to make the process available to non-EEO individuals looking into EEO internal process. 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 to 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.



Frances Castro
Project / Program Manager

2/16/17

Date



Manuel Mora
Information Security Manager


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: 2017.03.17 16:48:32 -06'00'

Date



Matthew Myers
Senior Agency Official for Privacy

Date



Diana Forti
Reviewing Official

5/9/17

Date