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

Privacy Impact Assessment (PIA)

For the

Safety & Security Division

Date: February 16, 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 / Safety & Security Division		**System/Project Acronym: GSS / SSD**
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: Aaron Haynes Title: Chief, Safety & Security Division Division: Safety & Security Division Telephone: 915-832-4782
Privacy Office or Designee Name: Matthew Myers Title: Chief Legal Counsel 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.

Personnel Security (PERSEC) program:

IBWC Form 063, Request for Suitability Action is filled out by the Human Resources Office (HRO) who provides the form to the Safety and Security Division (SSD). Our office uses this information to establish an Electronic Questionnaire for Investigation Processing (e-QIP) account. The e-QIP system is managed and operated by the Office of Personnel Management's (OPM) Federal Investigative Service (FIS).

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.

Date of birth; social security number; family member information; court documents and information; investigation records; security clearance information; criminal history; passport information; credit report; financial information; military service information; citizenship information; home address; education information; employment activities/conduct; drug usage information; mental history; and medical information. All information is used during suitability and national security investigations and adjudications.

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.)

Used solely for conducting background investigations, specifically suitability and national security.

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.)

In-person; mail; telephonically; email; fax; and hard copy.

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.

Office of Personnel Management-Federal Investigative Service; Federal Bureau of Investigation; Department of Defense; Defense Security Service; all Federal agencies of previous employment

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.

Date of birth; social security number; family member information; court documents and information; investigation records; security clearance information; criminal history; passport information; credit report; financial information; military service information; citizenship information; home address; education information; employment activities/conduct; drug usage information; mental history; and medical information. All information is used during suitability and national security investigations and adjudications.

Used solely for conducting background investigations, specifically suitability and national security.

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):

Yes. However, if they refuse, they can be denied employment with the Federal government per 5 CFR 731.

☐ 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.

Federal Investigative Service; other agencies requesting background investigation information; SSD personnel to include the Chief Security Officer (CSO), Assistant Chief Security Officer (ACSO), Security Specialist-PERSEC, and the Security Assistant.

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

Access to the information stored in the SSD is controlled by the Chief Security Officer. Access is only given to SSD personnel who have a need to know, have been granted access by OPM-FIS, Electronic Questionnaire for Investigation Processing (e-QIP) and have successfully completed the background investigation required for such access. INV Form 70B is submitted to the OPM-FIS for access to the Central Verification System (CVS) and the Personnel Investigation Processing System (PIPS).

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.

Yes. All security personnel assigned to PERSEC duties within every agency have access to CVS, PIPS and e-QIP

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.

Both CVS, e-QIP and PIPS are controlled by OPM-FIS. They establish the policy and control who is granted access to the systems.

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.

Both CVS, e-QIP and PIPS are controlled by OPM-FIS. They establish the policy and control who is granted access to the systems.

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?

Internally no contractors have access or a need for access to these systems. However, CVS, e-QIP and PIPS are controlled by OPM-FIS. They establish the policy and control who is granted access to the systems.

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?

The hard copy and data entry of information at agency level is verified by the PERSEC personnel assigned to the SSD. Information entered by OPM-FIS is controlled by them.

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

OPM-FIS monitors access to CVS, e-QIP and PIPS. Internally, hard-copy documents and digital records are stored in secure safes and on the shared drive that is only accessible by SSD 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.

Data in CVS, e-QIP, and IPS is retrieved by entering a social security number and name. Sometimes a date of birth and place of birth is required.

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?

Complete background investigation files, fingerprint results, adjudication status, case status, security clearance information. These files are destroyed for employees that are no longer with the agency.

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.

Security 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?

N/A

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.

To access the digital files we are required to use PIV/logical access with an approved government certificate.

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.

OPM-FIS monitors the use of CVS, e-QIP and PIPS. Internally, IMD monitors access to IBWC GSS network.

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 IBWC GSS network and physical safes. 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. The results of this PIA will compel the IMD to create a more secure environment to store and maintain forms with PII on them and train personnel on encrypting data that may continue to be sent via email.

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.

AARON HAYNES Digitally signed by AARON HAYNES
Date: 2017.02.16 11:18:38 -07'00'

Aaron Haynes
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: 2017.03.17 17:22:19 -06'00'

Zenon Mora
Information Security Manager **Date**

Matthew Myers
Senior Agency Official for Privacy **Date**

5/9/17

Diana Forti
Reviewing Official **Date**