



United States International Boundary and Water Commission

Protection of Sensitive Information Acknowledgement

A Privacy Impact Assessment (PIA) has been performed for the Office of Human Resource Department (HRD).

The Office of HRD has been given instruction and/or guidance from:

USIBWC Directives – Information Technology Policy and Procedures
(Located at: <http://www.ibwc.state.gov/Directives/IndexPage3.html>)

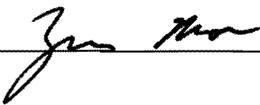
-or-

Annual Information Security Awareness Training (given verbally or taken electronically from the Information Security Cabinet located in shared GroupWise Cabinets)

on how to store and protect all Personally Identifiable Information (PII) and For Official Use Only (FOUO) information in any transferable media format by the Information Management Division (IMD) or Information System Security Officer (ISSO).

The office of HRD now accepts and acknowledges all responsibility for maintaining and protecting PII and FOUO information in any transferable media format.

IMD Supervisor Signature



Date

9/27/07

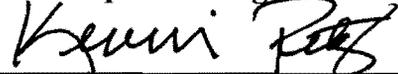
ISSO Signature



Date

9/27/07

Office Supervisor Signature



Date

09-27-07

United States International Boundary and Water Commission
Privacy Impact Assessment (PIA)

Name of Project: Human Resources Department (HRD) PIA
Bureau: USIBWC

Once the PIA is completed and the signature approval page is signed, please provide copies of the PIA to the following:

- USIBWC IT Security Manager
- USIBWC Privacy Act Officer

Do not email the approved PIA directly to the Office of Management and Budget email address identified on the Exhibit 300 form. One transmission will be sent by the OCIO Portfolio Management Division.

This PIA was performed on: April 11 2007

Also refer to the signature approval page at the end of this document.

A. CONTACT INFORMATION:

- 1) **Who is the person completing this document?** (Name, title, organization and contact information).
Rick Strackbein ISSO, (915) 832-4708
- 2) **Who is the system owner?** (Name, organization and contact information).
Matt Medor ISO, (915) 832-4130
- 3) **Who is the system manager for this system or application?** (Name, organization, and contact information).
Zenon Mora ISSM, (915) 832-4755
- 4) **Who is the IT Security Manager who reviewed this document?** (Name, organization, and contact information).
Zenon Mora ISSM, (915) 832-4755
- 5) **Who is the Bureau/Office Privacy Act Officer who reviewed this document?** (Name, organization, and contact information).
Tony Chavez (915) 832-4111
- 6) **Who is the Reviewing Official?** (According to OMB, this is the agency CIO or other agency head designee, who is other than the official procuring the system or the official who conducts the PIA).
Diana Forti CIO, (915) 832-4123

B. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals?

Yes (DOB, SSN, Names, Addresses)

a. Is this information identifiable to the individual¹?

(If there is **NO** information collected, maintained, or used that is identifiable to the individual in the system, the remainder of the Privacy Impact Assessment does not have to be completed).

Yes

b. Is the information about individual members of the public?

(If **YES**, a PIA must be submitted with the OMB Exhibit 300, and with the IT Security C&A documentation).

Employees as well as members of the public.

c. Is the information about employees? (If yes and there is no information about members of the public, the PIA is required for the USIBWC IT Security C&A process, but is not required to be submitted with the OMB Exhibit 300 documentation).

Yes

2) What is the purpose of the system/application?

To keep documentation and records on employees, administrative actions, and other human resource functions.

3) What legal authority authorizes the purchase or development of this system/application?

USIBWC

¹ "Identifiable Form" - According to the OMB Memo M-03-22, this means information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

C. DATA in the SYSTEM:

1) What categories of individuals are covered in the system?

DOB, SSN, Name, Race, Age, Gender, Occupation, work locations

2) What are the sources of the information in the system?

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

The information is taken from both the individual and other sources. Some information is taken from the individual, while other information is taken from the USIBWC Finance system, and remote field offices.

b. What Federal agencies are providing data for use in the system?

Department of interior, United States Department of Agriculture

c. What Tribal, State and local agencies are providing data for use in the system?

Only USIBWC

d. From what other third party sources will data be collected?

Other than NFC and USDA, none.

e. What information will be collected from the employee and the public?

Name, address, SSN, health benefits, background information

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than USIBWC records be verified for accuracy?

Most information is taken from the individual. If the individual is an existing employee then records from the finance system and previous records will be used to verify accuracy. If the individual is not an employee then background checks will be used to verify accuracy.

b. How will data be checked for completeness?

Examined by The HRO department for completeness when submitted

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

Once the information is entered into the system, the information will not be changed unless requested or a need exists.

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

Yes, a variety of HRO required forms are used

D. 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 aggregation from the information collected, and how will this be maintained and filed?

No, data stays in database. If data is printed then once the information is no longer needed then it is shredded. Hard copy files stored in locked file cabinets.

3) Will the new data be placed in the individual's record?

Yes

4) Can the system make determinations about employees/public that would not be possible without the new data?

No

5) How will the new data be verified for relevance and accuracy?

Data is verified by the individual submitting required forms or documentation and other resources may be used to verify accuracy.

6) If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

IT security software, IMD, locked file cabinets, video cameras (no video recording takes place) monitored by the Human Resources staff.

7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.

Hardcopy protection encompasses proper protections, electronic protections are being implemented.

8) How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

Electronic file storage and locking file cabinets

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

Various reports can be produced from this data. The use of the information is for required HRO procedures and official functions. Access is given to all HRO personnel, Willie S. from FSD, annual auditors, EEO, and Legal.

10) What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent.)

Individual have rights to decline however their requests will not get processed.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

N/A

2) What are the retention periods of data in this system?

5 years minimum and indefinitely.

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?

National archives

4) Is the system using technologies in ways that the USIBWC has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

No

5) How does the use of this technology affect public/employee privacy?

N/A

6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

Yes the system provides the ability to locate an individual by their documented work location

7) What kinds of information are collected as a function of the monitoring of individuals?

Employees work location, health history, credit history (if background check is performed), administrative actions as well as various other information.

8) What controls will be used to prevent unauthorized monitoring?

IT security encryption software, locked file cabinets and restricted network shares.

9) Under which Privacy Act systems of records notice does the system operate? Provide number and name.

Title 5

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

Unknown

F. ACCESS TO DATA:

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

If necessary the IMD, and all HRO personnel

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

No access if given to any user. Access only granted by need-to-know

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

No access is given to any user unless it is the individuals own records.

4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials)

Locked file cabinets, need-to-know basis, electronic security.

5) **Are contractors involved with the design and development of the system and 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?**

No

6) **Do other systems share data or have access to the data in the system? If yes, explain.**

NFC has access to a system shared by USIBWC HRO, by financial reports only. NFC does not have direct access to the system.

7) **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

HRO office personnel and IMD

8) **Will other agencies share data or have access to the data in this system (Federal, State, Local, Other (e.g., Tribal))?**

NFC

9) **How will the data be used by the other agency?**

Financial and payroll purposes.

10) **Who is responsible for assuring proper use of the data?**

HRO personnel IMD and USIBWC

In Conclusion:

The Human Resources Department does encompass adequate controls that protect sensitive information while in storage, transit and additionally while being utilized. The employees in the Human Resources Department have been identified as having enhanced security training needs, and will attend tailored additional refresher security training.

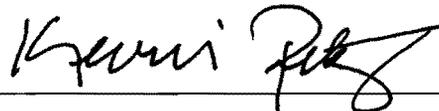
See Attached Approval Page

The Following Officials Have Approved this Document

1) Department Supervisor

Name: KEYIN PETZ

Title: HR DIRECTOR

Signature:  Date: 09/27/07

2) IT Security Manager

Name: ZENON MONA

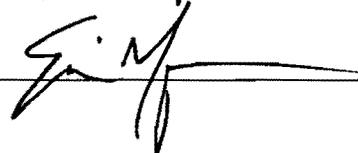
Title: Supv. IT Specialist

Signature:  Date: 9/27/07

3) Privacy Act Officer

Name: ERIC MEZA

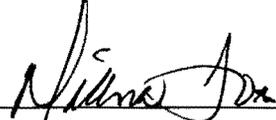
Title: Paralegal Specialist / FOIA Officer

Signature:  Date: 9/28/07

4) Reviewing Official

Name: DIANA FORTI

Title: CHIEF ADMINISTRATIVE OFFICER / CID

Signature:  Date: 10/1/07