This document is scheduled to be published in the Federal Register on 12/07/2015 and available online at **http://federalregister.gov/a/2015-29531**, and on **FDsys.gov**

7010-01

==========

INTERNATIONAL BOUNDARY AND WATER COMMISSION, UNITED STATES AND MEXICO

Privacy Act of 1974; Establishment of a New System of Records

AGENCY: United States Section, International Boundary and Water Commission (USIBWC), United States and Mexico

ACTION: Proposed establishment of a new Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974, as amended (5 U.S.C. 552a), the USIBWC is issuing public notice of its intent to establish a new Privacy Act system of records, DOI-84, "Interior Business Center Datamart."

DATES: Comments must be received by January 2, 2016.

ADDRESSES: Any persons interested in commenting on this new, proposed system of records may do so by submitting comments in writing to the Legal Department, Senior Agency Officer for Privacy, Matthew Myers, U.S. IBWC, 4171 N. Mesa, C-100, El Paso, TX 79902, or by e-mail to Matthew.Myers@ibwc.gov

FOR FURTHER INFORMATION CONTACT: Z. Mora, Chief, Information Management Division, Administration Department, 4171 N. Mesa, C-100, El Paso, TX 79902 or by e-mail at Z.Mora@ibwc.gov

SUPPLEMENTARY INFORMATION: The information contained in Datamart is derived from two existing systems covered by Privacy Act Systems of Records Notices: Federal Personnel and Payroll System (FPPS) covered by DOI-85, ``Payroll, Attendance, Retirement, and Leave Records'' and Federal Financial System

(FFS) covered by DOI-90, ``Federal Financial System,'' as well as associated systems. The purpose of the Datamart is to provide a data warehouse that allows appropriate users to access FPPS and FFS data through a core reporting tool, Hyperion. The reports may be pre-formatted or ad hoc, and are available to appropriate users from the Department of the Interior or appropriate individuals from other Federal agencies, as detailed in the routine uses. This notice will be effective as proposed at the end of the comment period unless comments are received which would require a contrary determination. The USIBWC will publish a revised notice if changes are made based upon a review of comments received.

Dated: October 8, 2015.

Matthew Myers,

Chief Counsel/Secretary Acting Privacy Act Officer.

System Name:

Interior, Interior Business Center Datamart, DOI-84.

SYSTEM LOCATION:

Records are located at the Interior Business Center, U.S. Department of the Interior, 7301 West Mansfield Avenue, Denver, CO 80235.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEMS:

(1) Current and former employees of the USIBWC.

(2) Current and former emergency workers of the USIBWC.

(3) Current and former volunteers within the USIBWC (volunteers).

(4) Current and former contractors within the USIBWC (contractors).

(5) Individuals identified as emergency contacts for the above employees, emergency workers, and volunteers.

(6) Individual and corporate vendors who do business with the USIBWC. (Only records containing personal information relating to individuals are subject to the Privacy Act.)

CATEGORIES OF RECORDS IN THE SYSTEM:

Employee (and emergency worker, volunteer, contractor and vendor) name, address, phone numbers, birth date; employee (and emergency worker and volunteer) emergency contact information (including name, address, phone numbers and relationship to individual), Social Security Number and organizational code; employee common identifier (ECI); vendor Taxpayer Identification Number; vendor code or number; employee ethnicity/race, pay rate, grade, length of service, individual's pay and leave records; time and attendance records, leave request records, allowances and cost distribution records; employee deductions for Medicare, Old Age Survivor and Disability Insurance (OASDI), bonds, Federal Employees' Group Life Insurance (FEGLI), union dues, taxes, allotments, quarters, retirement, charities, health benefits, Flexible Spending Account, Long Term Care, and Thrift Savings Fund contributions; employee awards, shift schedules, pay differentials, tax lien data, commercial garnishments and child support and/or alimony wage assignments; related payroll and personnel data. Also included is information on debts owed to the government as a result of overpayment, refunds owed or a debt referred for collection on an employee, emergency worker or contractor.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

31 U.S.C. 3512, et seq.; 5 U.S.C. 5101, et seq.; Pub. L. 97-255; Office of Management and Budget Circular A-127.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

The primary use of records in the system is to provide a repository for data from FPPS (Federal Personnel Payroll System) and FFS (Federal Financial System) that allows agencies to query the data in order to produce required reports in support of fiscal operations and personnel payroll processing.

Disclosure outside the USIBWC may be made:

(1) To other Federal agencies to produce required reports, in support of their fiscal and personnel/payroll processing.

(2) (a) To any of the following entities or individuals, when the circumstances set forth in paragraph (b) are met:

(i) The U.S. Department of Justice (DOJ);

(ii) A court or an adjudicative or other administrative body;

(iii) A party in litigation before a court or an adjudicative or other administrative body; or

(iv) Any USIBWC employee or USIBWC emergency worker acting in his or her individual capacity if USIBWC or DOJ or the DOI emergency worker's agency has agreed to represent that individual or pay for private representation of the individual;

(b) When:

(i) One of the following is a party to the proceeding or has an interest in the proceeding:

(A) USIBWC or any component of USIBWC;

(B) Any USIBWC emergency worker's agency;

(C) Any other Federal agency appearing before the Office of Hearings and Appeals;

(D) Any USIBWC employee or USIBWC emergency worker acting in his or her official capacity;

(E) Any USIBWC employee or USIBWC emergency worker acting in his or her individual capacity if USIBWC or DOJ or the USIBWC emergency worker's agency has agreed to represent that individual or pay for private representation of the individual;

(F) The United States, when DOJ determines that USIBWC or any USIBWC emergency worker's agency is likely to be affected by the proceeding; and

(ii) USIBWC or any DOI emergency worker's agency deems the disclosure to be:

(A) Relevant and necessary to the proceeding; and

(B) Compatible with the purpose for which the records were compiled.

(3) To appropriate agencies, entities, and persons when:

(a) It is suspected or confirmed that the security or confidentiality of information in the system of records has been compromised; and

(b) The USIBWC has determined that as a result of the suspected or confirmed compromise there is a risk of harm to an economic or property interest, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and

(c) The disclosure is made to such agencies, entities and persons who are reasonably necessary to assist in connection with the USIBWC’s efforts to respond to the suspected or confirmed compromise and prevent, minimize or remedy such harm.

(4) To a congressional office in response to a written inquiry that an individual covered by the system, or the heir of such individual if the covered individual is deceased, has made to the office.

(5) To any criminal, civil or regulatory law enforcement authority (whether federal, state, territorial, local, tribal or foreign) when a record, either alone or in conjunction with other information, indicates a violation or potential violation of law--criminal, civil or regulatory in nature, and the disclosure is compatible with the purpose for which the records were compiled.

(6) To an official of another Federal agency to provide information needed in the performance of official duties related to reconciling or reconstructing data files or to enable that agency to respond to an inquiry by the individual to whom the record pertains.

(7) To Federal, state, territorial, local, tribal or foreign agencies that have requested information relevant or necessary to the hiring, firing or retention of an employee or contractor, or the issuance of a security clearance, license, contract, grant or other benefit, when the disclosure is compatible with the purpose for which the records were compiled.

(8) To representatives of the National Archives and Records Administration to conduct records management inspections under the authority of 44 U.S.C. 2904 and 2906.

(9) To state and local governments and tribal organizations to provide information needed in response to court order and/or for discovery purposes related to litigation, when the disclosure is compatible with the purpose for which the records were compiled.

(10) To an expert, consultant or contractor (including employees of the contractor) of DOI that performs services requiring access to these records on DOI's behalf to carry out the purposes of the system.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Records maintained in the Datamart are electronic and contain information from source systems. They are stored in magnetic media at the central computer processing center. All NIST guidelines, as well as Departmental and OMB guidance are followed concerning the storage of the records.

RETRIEVABILITY:

Records may be retrieved by entries reflecting the various categories of records in the system including name of individual, name of emergency contact, Social Security Number, Tax Identification Number, vendor code or number, date of birth, organizational code, etc.

SAFEGUARDS:

Electronic records are maintained with safeguards meeting all appropriate statutory and regulatory guidelines, as well as Departmental guidance addressing the security requirements of Departmental Privacy Act Regulations (43 CFR 2.51) for automated records, and with Office of Management and Budget, and NIST. Further, agency officials only have access to records pertaining to their agencies.

(1) Physical security: Computer systems are maintained in locked rooms housed within secure USIBWC buildings.

(2) Technical Security: Electronic records are maintained in conformity with Office of Management and Budget and USIBWC guidelines reflecting the implementation of the Federal Information Security Management Act. The

electronic data are protected through user identification, passwords, database permissions, encryption and software controls. Such security measures establish different degrees of access for different types of users. An audit trail is maintained and reviewed periodically to identify unauthorized access. A Privacy
Impact Assessment was completed to ensure that Privacy Act requirements and personally identifiable information safeguard requirements are met.

(3) Administrative Security: All USIBWC and contractor employees with access to Datamart are required to complete Privacy Act, Federal Records Act and IT Security Awareness training prior to being given access to the system, and on an annual basis thereafter. In addition, Federal employees supervise and monitor the use of Datamart.

RETENTION AND DISPOSAL:

Records contained in this system are documented as items 1400 and 7554 of the Department of the Interior, Office of the Secretary's pending records schedule.

SYSTEM MANAGER AND ADDRESS:

Chief, Applications Management and Technical Services Branch, Interior Business Center, U.S. Department of the Interior, 7301 West Mansfield Avenue, Denver, CO 80235-2230.

NOTIFICATION PROCEDURES:

Inquiries regarding the existence of records should be addressed to the System Manager. The request must be in writing, signed by the requester, and meet the requirements of 43 CFR 2.60, which requires writing PRIVACY ACT INQUIRY prominently on your envelope and correspondence.

RECORDS ACCESS PROCEDURES:

A request for access should be submitted to the System Manager at the above address. It must be submitted in writing, signed by the requester, and meet the requirements of 43 CFR 2.63, which requires writing PRIVACY ACT REQUEST FOR ACCESS prominently on the envelope and the front of the request.

CONTESTING RECORDS PROCEDURES:

A petition for amendment should be addressed to the System Manager. The request must be in writing, signed by the requester, and meet the content requirements of 43 CFR 2.71, which include stating the reasons why the petitioner believes the record is in error, and the changes sought.

RECORD SOURCE CATEGORIES:

The source data for the system comes from FPPS and FFS.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

[FR Doc. E8-29019 Filed 12-5-08; 8:45 am]

BILLING CODE 4310-RK-P

[FR Doc. 2015-29531 Filed: 12/4/2015 8:45 am; Publication Date: 12/7/2015]