U.S. DEPARTMENT OF LABOR

Office of Worker's Compensation Programs

DIVISION OF FEDERAL EMPLOYEES' COMPENSATION
INTEGRATED FEDERAL EMPLOYEES' COMPENSATION SYSTEM (iFECS)
DOL-OWCP-M-008

PRIVACY IMPACT ASSESSMENT

VERSION 7.0

JUNE 2012

CONTROLLED UNCLASSIFIED INFORMATION

DOCUMENT CHANGE HISTORY

Date	Filename / Version #	Author	Revision Description
10/04	1.0	Initial Version using NIST SP 800-30/DOL CSH format	DFEC/OWCP
11/05	1.1	Updated Document using most current template	DFEC/OWCP
11/06	November 2006	Annual update.	DFEC/OWCP
11/07	2.0	Annual update. Updated document using revised template.	DFEC/OWCP
12/07	2.1	Revised per comments received from DITMS on 12/18/07.	DFEC/OWCP
01/08	2.2	Updated document using revised template from 12/07.	DFEC / OWCP
03/08	2.3	Updated to conform to changes in the SCW.	DFEC / OWCP
04/08	3.0	Revised per comments received from OCIO on 03/03/08.	DFEC / OWCP
06/09	4.0	Updated document using revised template 1.5.	DFEC / OWCP
05/10	5.0	Annual Update. Updated document using revised template 1.6.	DFEC / OWCP
06/11	6.0	Annual Update.	DFEC / OWCP
06/12	7.0	Annual Update. Updated document using revised template, August 2011.	DFEC / OWCP

DOCUMENT REVIEW HISTORY

Date	Version #	Reviewers
06/11	6.0	DFEC / OWCP
06/12	7.0	DFEC / OWCP

TABLE OF CONTENTS

PRIVACY IMPACT ASSESSMENT QUESTIONNAIRE

1.1. OVERVIEW

In accordance with Department of Labor (DOL) guidelines, the Office of Workers' Compensation Programs (OWCP) Division of Federal Employees' Compensation (DFEC) conducted a Privacy Impact Assessment (PIA) on the integrated Federal Employees' Compensation System (iFECS).

iFECS is a major application that provides a case management system to support DFEC core business functions in administering the Federal Employees' Compensation Act. iFECS includes the iFECS system and three sub-components, the Agency Query System (AQS), the Claimant Query System (CQS) and the Employees' Compensation Operations and Management Portal (ECOMP). iFECS is a three-tier application that was established to provide the Federal Employees' Compensation Act (FECA) with an automated case management system.

The OWCP, in conjunction with the Office of the Chief Information Officer (OCIO), has determined that iFECS processes privacy information. As such, this document has been prepared to describe the information collected by iFECS; what it is used for; who has access to the information; how the information can be corrected; and in general terms how the information is secured.

iFECS provides data processing for DFEC application systems, program management systems, DFEC financial management and other administrative systems, and decision support systems supporting DFEC users nationwide. Data on entitlement, benefit payment status and attorney fees that is maintained on the iFECS is available in accordance with the Privacy Act to user organizations via telephone and in paper/electronic formats.

The DFEC District Offices (DOs) are located in: Boston, MA; New York, NY; Philadelphia, PA; Jacksonville, FL; Cleveland, OH; Chicago, IL; Kansas City, MO; Dallas, TX; Denver, CO; San Francisco, CA; Seattle, WA; Washington, DC and Hearings and Reviews. The DOs process compensation claims and medical bills, and authorize wage replacement and medical benefits.

This PIA covers the entire compensation process for the FECA program except for medical bill payment and pre-authorization services which have been outsourced to a medical billing contractor. Those parts of the process are addressed in the PIA for the Central Bill Process (CBP).

DOL, in compliance with federal privacy laws, regulations, and directives, is responsible for ensuring PII that in-house agencies collect, store, and transmit is properly protected.

In accordance with DOL guidelines, the OWCP DFEC conducted a PIA on iFECS. iFECS is a major application that provides an online case management system to support DFEC core business functions in administering the Federal Employees' Compensation Act.

1.2. CHARACTERIZATION OF THE INFORMATION

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, or technology being developed.

Specify whether the system collects personally identifiable information (PII) on DOL employees, other federal employees, contractors, members of the public (U.S. citizens), foreign citizens, or minor children.

iFECS collects PII on individuals and/or their survivors who file claims seeking benefits under the FECA by reason of injuries sustained while in the performance of duty. The FECA applies to all civilian federal employees, including various classes of persons who provide or have provided personal service to the government of the United States, and to other persons as defined by law, such as state or local law enforcement officers who were injured or killed while assisting in the enforcement of federal law and their survivors. In addition, the FECA covers employees of the Civil Air Patrol, Peace Corps Volunteers, Job Corps students, Volunteers in Service to America, members of the National Teachers Corps, certain student employees, members of the Reserve Officers Training Corps, certain former prisoners of war, and employees of particular commissions and other agencies.

In addition to these individuals, the system contains records of medical providers, attorneys representing claimants, rehabilitation counselors, nurses, and other health care professionals who provide information in support of compensation claims.

- What are the sources of the PII in the information system?

PII is provided to the agency in a variety of ways including:

- Reports of injury by the employee and/or employing agency;
- Claim forms (CA-1, CA-2, CA-5, etc.) filed by or on behalf of injured federal employees or their survivors seeking benefits under the FECA. A list of forms can be found at the following link:
  http://www.dol.gov/owcp/dfec/regs/compliance/forms.htm
- Forms authorizing medical care and treatment;
- Other medical records and reports;
- Bills and other payment records;
- Compensation payment records;
- Formal orders for or against the payment of benefits;
- Transcripts of hearings conducted;
- Any other medical, employment, or personal information submitted or gathered in connection with the claim.
- Information relating to dates of birth, marriage, divorce, and death;
- Notes of telephone conversations conducted in connection with the claim;

- Information relating to vocational and/or medical rehabilitation plans and progress reports;
- Records relating to court proceedings, insurance, banking and employment;
- Articles from newspapers and other publications;
- Information relating to other benefits (financial and otherwise) the claimant may be entitled to;
- Information received from various investigative agencies concerning possible violations of Federal civil or criminal law.

Consumer credit reports on individuals indebted to the United States, information relating to the debtor's assets, liabilities, income and expenses, personal financial statements, correspondence to and from the debtor, information relating to the location of the debtor, and other records and reports relating to the implementation of the Federal Claims Collection Act (as amended), including investigative reports or administrative review matters. Individual records listed here are included in a claim file only insofar as they may be pertinent or applicable to the employee or beneficiary.

- What is the PII being collected, used, disseminated, or maintained?

  - First and/or last name
  - Date of birth
  - Social Security Number (SSN)
  - Residential address
  - Personal phone numbers (e.g., phone, fax, cell)
  - Mailing address (e.g., P.O. Box)
  - Medical information including physician’s notes
  - Medical record number
  - Financial account information and/or number (e.g., checking account number, PIN, retirement, investment account)
  - Certificates (e.g., birth, death, marriage)
  - Legal documents or notes (e.g., divorce decree, criminal records)
  - Employment Records
  - Compensation Payment Records
  - Survivor Eligibility Data, (e.g., relationship marriage, divorce, death)
  - Wage/Salary Information
  - Government Benefits data

- How is the PII collected?

  The FECA benefit process is initiated when a claimant (federal employee or dependent) submits a notice of injury, occupational disease, or death form to their respective Agency of employment. These claims can be broken into two main areas: (1) Medical, which includes disability and death claims, and (2) compensation, which is to reclaim lost wages from injury, disability, or disease.

  For medical claims:

  In disability cases, the appropriate forms are:
  - CA-1, Federal Notice of Traumatic Injury and Claim for Continuation of Pay/Compensation
  - CA-2, Notice of Occupational Disease and Claim for Compensation
  - CA-7, Claim for Compensation on Account of Traumatic Injury or Occupational Disease

  In death cases, the appropriate forms are:
  - CA-5, Claim for Compensation by Widow, Widower, and/or Children
  - CA-5b, Claim for Compensation by Parents, Brothers, Sisters, Grandparents, or Grandchildren
  - CA-6, Official Superior's Report of Employee's Death

  For compensation claims, the appropriate forms are:
  - CA-7, for Compensation on Account of Traumatic Injury or Occupational Disease
  - CA-16, Request for Examination and/or Treatment or Form
  - CA-20, Attending Physician’s Report

  Once the claim form has been received by the employing agency, the employing agency completes the remaining information and sends the form to the applicable DOL District Office for processing based on the geographical location of the employing agency. The forms may be submitted in paper form or, if a claim is created by a claimant from a federal agency that has been established as an Electronic Data Interchange (EDI) trading partner, it is submitted to the OWCP through EDI.

  At the District Office, manual claimant information from the claim form is entered into the iFECS by a Case Create Clerk. iFECS automatically assigns a unique case number for the claim. The Case Create Clerk then sends the claim form to the Imaging Operator for imaging. If the information is received via EDI, at noon each day those files are picked up from a secure server location, put through a series of validation checks, and finally populate the forms in iFECS. The Case Create Clerk can then see those claims and reviews them before they are assigned a case number by the system.

The Imaging Operator scans the hardcopy claim form into iFECS to produce a digital image of the form. After the case is created and assigned a case number (using either the paper cases or EDI cases), the case is then routed to a Claims Examiner (CE) for review

Additional PII will be collected in the form of medical records, correspondence, etc. during the course of the claim by claims examiners in the various DFEC offices and by the medical bill payment contractor. This input may come from a variety of health care professionals including contract nurses, rehabilitation counselors, doctors, etc.

The DFEC contractor receives paper medical bills from medical providers, claimants, and DFEC District Offices. They also receive paper and electronic pharmacy bills from providers and claimants. Contract staff prepares and organizes these documents at contractor facilities. The images of the documents are stored on a server. All inbound and outbound call reference notes are also transcribed and are available electronically to support the bill payment process. A secured Web portal is provided to allow providers and claimants on-line read only access to information about their claims.

Some information from case forms that were described above is received by DFEC from the medical bill payment contractor systems electronically for the purpose of establishing the claimant records in iFECS.

- How will the information be checked for accuracy?

  For EDI records the system puts them through three phases of edit and validation checks before the data is available in iFECS. If the record does not pass those tests, it is rejected and the agency notified that the record needs to be corrected and resubmitted. In addition, once a record is received in iFECS, the Case Create Clerk reviews the data before the case number is assigned.

  During case development, the Claims Examiner reviews the accuracy of the information that was entered by the Case Create Clerk or in the EDI file by comparing the claim form to the information in iFECS. If the information is not correct, the Claims Examiner makes the corrections. Access controls are in place within iFECS to ensure that the Claims Examiner who monitors the file does not have access to create cases.

  The images of the documents received by medical bill payment contractor are electronically indexed, verified, and quality checked before being transmitted to DOL and to contactor State Healthcare for adjudication and payment processing.

- What specific legal authorities, arrangements, and/or agreements defined the collection of information?

OWCP has been authorized by Congress (Public Law 103-333: Departments of Labor, Health and Human Services, and Education, and Related Agencies Appropriations Act, 108 Stat. 2539, September 30, 1994) to require persons who file notices of injury and/or claims for compensation under the FECA and its extensions to disclose certain identifying information, including SSN. Consequently, applicable regulations concerning the filing of a notice of injury and claim for compensation, including 20 C.F.R. §§ 10.100 (traumatic injury), 10.101 (occupational disease), and 10.105 (death), have been amended to expressly require the reporting of the injured worker's SSN. These regulations were published on November 25, 1998, and were effective January 4, 1999. See 63 F.R. 65284.

- Privacy Impact Analysis

  There are many potential risks when medical information is recorded about an individual, such as identity theft, certain types of insurance coverage being refused if certain medical information became public, loss of employment, etc. In particular, the risk of PII being disclosed inadvertently when information is being passed between medical offices, rehabilitation counselors, other medical staff and DFEC is taken very seriously. DFEC understands its obligation to safeguard this information to prevent any of the potential risks from being realized and has established policies and procedures to safeguard this information. Throughout the remainder of this document examples of those safeguards have been explained to illustrate this commitment to prevention of PII being compromised.

  In addition to the safeguards in place internally, DFEC requires its medical bill payment contractor's operation to be in full compliance with Federal security guidance to ensure proper safeguards are in place to prevent the accidental release of information that has been entrusted to the organization.

1.3. USES OF THE PII

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

- Describe all the uses of the PII

  DFEC uses the collected PII as critical information for the purposes of managing the claimant's case and successfully fulfilling the mission.

  iFECS operations provide the following functions which in some part depend on PII:

  - Input and process claims
  - Conduct correspondence with claimants, attorneys, and various medical personnel to determine the eligibility of the claim
  - Determine whether a claim is eligible or not, and notify the claimant
  - Periodically update claimant and medical information to determine continued eligibility
  - Calculate the amount of benefits the claimant is eligible for
  - Receive electronic file of approved payments from contractor for transmission to the Treasury Department
  - Disburse benefit payments to claimants or their beneficiaries
  - Review pre-authorization requests for medical procedures
  - Support rehabilitation training and counseling
  - Conduct hearings and reviews when a claimant or their representative has filed an appeal
  - Provide statistics for quality reviews including utilization review and fraud and abuse detection
  - Recover funds that have been disbursed in error or where an overpayment has been made

- What types of tools are used to analyze data and what type of data may be produced?

  Data mining and some pattern recognition are used to look for instances of potential fraud, as well as for reporting purposes, i.e. to determine if performance goals are being met.

- Will the system derive new data, or create previously unavailable data, about an individual through aggregation of the collected information?

  No.

- If the system uses commercial or publicly available data, please explain why and how it is used.

  iFECS employs the NTIS SSA Death Master File (DMF) to check for decedents. iFECS also uses American Medical Association (AMA) physician data for selection of Independent Medical Examiners.

- Privacy Impact Analysis

  All system users are required to read and sign the Rules of Behavior before being granted access to the system. The iFECS uses least privilege principles to ensure that only those who need access to the data to fulfill the agency's mission are given access in addition to the authentication controls discussed above.

  The system maintains only PII that is necessary and relevant to accomplish the purpose for which it is being collected.

1.4. RETENTION

The following questions are intended to outline how long information will be retained after the initial collection.

- How long is information retained in the system?

  - FECA Claimant Case Files: All case files and automated data pertaining to a claim are destroyed 15 years after the case file has become inactive. Case files that have been scanned to create electronic copies are destroyed after the copies are verified. Automated data is retained in its most current form only, however, and as information is updated, outdated information is deleted. Some related financial records are retained only in electronic form, and destroyed 6 years and 3 months after creation or receipt.

  - Records for Physicians and Health Care Providers Excluded under the Federal Employees' Compensation Act: File is retained in the office for three years after the debarment action is final and then transferred to the Federal Records Center, and destroyed thirty years after the debarment action is final. Where the period of exclusion is defined as a set period of time, the file will be retained two years after the period of exclusion expires (or the individual is otherwise reinstated), then transferred to the Federal Records Center, and destroyed thirty years after the debarment action is final.

  - Rehabilitation Files: All rehabilitation files are merged with the FECA case file (see DOL/GOVT-1) at the conclusion of the rehabilitation effort and are retained consistent with the retention schedule for the case files.

  - Rehabilitation Counselor Case Assignment: All case files and automated data pertaining to the OWCP rehabilitation counselors/nurses are maintained for two years following the termination of the contract.

- Has the retention schedule been approved by the DOL agency records officer and the National Archives and Records Administration (NARA)?

  Yes. The Archivist of the United States signed the “Request for Records Disposition Authority”, Job Number: N1-271-02-01 on April 30, 2004.

- How is it determined that PII is no longer required?

  The OWCP programs, under which PII records are collected and processed, are authorized by Congress to collect such information. Because these records are part of the official record that justifies the compensation decisions made by OWCP, they are required to be maintained as part of the audit record for the agency.

- What efforts are being made to eliminate or reduce PII that is collected, stored or maintained by the system if it is no longer required?

  PII is only stored on the system for a period of up to seven years. After that, non-active database records are copied to tape and the archived records are stored at a separate backup facility.

- Privacy Impact Analysis

  The iFECS is required to maintain the paper record for the interval indicated by the Archivist of the United States. The paper files are maintained in a secure location within the DFEC offices. Once the file is eligible to be shipped to the Federal Records Center, it is sent via tracked packages which are labeled appropriately. The electronic records are secured with numerous security controls.

1.5. INTERNAL SHARING AND DISCLOSURE

The following questions are intended to define the scope of sharing within the Department of Labor.

- With which internal organization(s) is the PII shared, what information is shared, and for what purpose?

  Electronic case records can be requested by the following organizations outside of the OWCP program for auditing purposes: the DOL Office of Inspector General (OIG) and the Office of the Chief Financial Officer (OCFO) for audit purposes; and the Office of the Solicitor (SOL) for litigation support.

- How is the PII transmitted or disclosed?

  Access to data is provided via "read only" auditor user accounts for temporary periods required by the auditors. If any PII has to be transmitted to an auditor outside the DOL firewall, it is done via encrypted E-Mail attachment, password protected file or CD.

- Privacy Impact Analysis

  The sharing of data with internal users is limited to SOL for litigation support; and the OIG and OCFO and their designated auditors. All auditors are required to sign strict non-disclosure agreements, read and sign Rules of Behavior and complete security screening before they are authorized to access any data. The information is being shared with auditors and the SOL for civil or criminal law enforcement.

  The PII is protected by encryption while it is transmitted from the contractor to OWCP.

1.6. EXTERNAL SHARING AND DISCLOSURE

The following questions are intended to define the content, scope, and authority for information sharing external to DOL which includes federal, state and local government, and the private sector.

- With which external organization(s) is the PII shared, what information is shared, and for what purpose?

  Because of the nature of the DFEC program, virtually all government entities that employed the claimant at the time of the occurrence or recurrence of the injury or occupational illness send information to or receive iFECS information via Connect:Direct, CD, EDI, or other electronic means in order to:

  - Initiate a claim
  - Verify chargebacks
  - Answer questions about the status of the claim
  - Consider rehire, retention or other actions the agency may be required to take
  - Permit the agency to evaluate its safety and health program

  As discussed earlier, DFEC receives documents from its CBP contractor for purposes of prior authorization and other claims management. Also, as part of its contract with OWCP, CBP prepares files for transmission to the U.S. Treasury for payments to be made. These payments are authorized and approved by the OWCP program office, so no transaction is completed without the intervention of authorized federal staff who confirms the payments.

  DFEC also prepares and transmits files to the U.S. Treasury for payments to be made to claimants.

  Claimant and Agency Worker's Compensation staff can access information on their own claim(s) via AQS/CQS. PII is also shared with the DOL contracted providers: field nurses, and Vocational Rehabilitation counselors. By calling DFEC's Interactive Voice Response (IVR) system, injured workers and their representatives may access information regarding case status and compensation payments.

- Is the sharing of PII outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the PII outside of DOL.

  Yes. All collection and sharing of data is for the purpose of providing benefits to claimants. It is covered by the following SORNs:

- DOL/GOVT-1 - Office of Workers' Compensation Programs, Federal Employees' Compensation Act File
- DOL/ESA-29 - Physicians and Health Care Providers Excluded under the FECA
- DOL/ESA-43 - Rehabilitation Files
- DOL/ESA-44 - Rehabilitation Counselor Case Assignment, Contract Management and Performance Files and FEC Field Nurses.

Authorization is granted via contracts, a Memorandum of Understanding (MOU) and/or an Interconnectivity Security Agreement (ISA) between OWCP/DFEC and the outside contactors or Agencies. MOUs/ISAs awaiting finalization are being tracked as a DFEC POA&M item.

- How is the information shared outside the Department and what security measures safeguard its transmission?

  Some information is shared via portable media (CD) and, as of April 2008, is encrypted via the DOL mandated encryption software. Additional ways of sharing the information are through Secure email or Connect:Direct. The transmission through Connect:Direct includes two factor authentication and encryption of the data.

  OWCP has selected the American National Standard Institute (ANSI) Accredited Standards Committee (ASC) X12 as its electronic messaging standard for all EDI transactions exchanged between DOL and its trading partners to create workers' compensation claims. The X12 Transaction Set 148, *Report of Injury, Illness or Incident*, version 003070, has been selected by OWCP as the electronic message format used to transmit the CA-1 and CA-2 form. Only EDI files with unique batch IDs, which consist of the trading partner code and date, will be accepted each day. The EDI file, containing the claims captured in 148 transaction sets, is deposited on a secure server through secure file transfer protocol (SFTP) or Connect:Direct. Each trading partner must submit the EDI file from a designated internet protocol (IP) address. This IP address must be validated by the Division of IT Management and Services (DITMS) prior to submission. IP addresses that have not been validated will not be allowed access to the DOL file transfer protocol (FTP) server.

  Connections to the IVR system, AQS/CQS, and ECOMP require authentication before the user can access any information about their own claim(s).

  The transmission of data to Treasury's Financial Management Service (FMS) is through a direct connection which includes two factor authentication and encryption of the data.

- Privacy Impact Analysis

  The external sharing of data is the required connections to Agencies and the Treasury's FMS.

  The transmission of data to Treasury's FMS is done through a direct connection which includes two factor authentication and encryption of the data. Since the connection is made through the OWCP network, an Interconnection Security Agreement is in place between OWCP and Treasury's FMS. In addition, an MOU between DOL and the U.S. Treasury Department is in place covering this connection. The data enables payments to be issued to claimants.

  The various Agencies use the data extracts and/or Chargeback information for billing, verification, and reporting purposes.

  As discussed above EDI connections require that the files be transmitted from specific IP addresses via Connect:Direct or SFTP.

  For transmissions via the direct connection between the GSS and CBP, the PII is protected by encryption while it is transmitted.

1.7. NOTICE

The following questions are directed at notice to the individual of the scope of PII collected, the right to consent to uses of said information, and the right to decline to provide information.

- Was notice provided to the individual prior to collection of PII?

  Privacy Act considerations are included on the back of the CA-1 and CA-2 claimant forms. Claimants are instructed to review the entire document before submitting the form

- Do individuals have the opportunity and/or right to decline to provide information?

  Yes, we have the following statement included in our claimant forms (CA-1 and CA-2):

  In accordance with the Privacy Act of 1974, as amended (5 U.S.C. 552a), you are hereby notified that:
  (1) The Federal Employees' Compensation Act, as amended and extended (5 U.S.C. 8101, et seq.) (FECA) is administered by the Office of Workers' Compensation Programs of the U.S. Department of Labor, which receives and maintains personal information on claimants and their immediate families.
  (2) Information which the Office has will be used to determine eligibility for and the amount of benefits payable under the FECA, and may be verified through computer matches or other appropriate means.
  (3) Information may be given to the Federal agency which employed the claimant at the time of injury in order to verify statements made, answer questions concerning the status of the claim, verify billing, and to consider issues relating to retention, rehire, or other relevant matters.
  (4) Information may also be given to other Federal agencies, other government entities, and to private-sector agencies and/or employers as part of rehabilitative and other return-to-work programs and services.
  (5) Information may be disclosed to physicians and other health care providers for use in providing treatment or medical/vocational rehabilitation, making evaluations for the Office, and for other purposes related to the medical management of the claim.
  (6) Information may be given to Federal, state and local agencies for law enforcement purposes, to obtain information relevant to a decision under the FECA, to determine whether benefits are being paid properly, including whether prohibited dual payments are being made, and, where appropriate, to pursue salary/administrative offset and debt collection actions required or permitted by the FECA and/or the Debt Collection Act.
  (7) Disclosure of the claimant's social security number (SSN) or tax identifying number (TIN) on this form is mandatory. The SSN and/or TIN), and other information maintained by the Office, may be used for identification, to support debt collection

efforts carried on by the Federal Government, and for other purposes required or authorized by law.
(8) Failure to disclose all requested information may delay the processing.

- Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

  As indicated in the previous question, OWCP has been authorized by law to collect certain information in order to process claims. The information is used only for the purposes of managing the Federal Employees' compensation claim. Claimants consent to this use of their information by signing the claimant form.

  OWCP has the following statements included in our claimant forms:

  Claim for Medical Reimbursement form OWCP 915 OMB No. 1240-0007
  "I certify that the information above is correct and that the reimbursement requested is for expenses paid by me for the treatment of my covered condition. I am aware that any person who knowingly makes any false statement or misrepresentation to obtain reimbursement from OWCP is subject to civil penalties and/or criminal prosecution.

  I authorize any provider named above to release information to the US Department of Labor, OWCP if necessary for the proper adjudication of this claim."

  Medical Travel Refund Request form OWCP 957 OMB No. 1240-0037
  "This report is authorized by the Federal Employees' Compensation Act (5 USC 8103(a)), the Black Lung Benefits Act (30 USC 901; 20 CFR 725.406 and 725.701) and the Energy Employees Occupational Illness Compensation Program Act of 2000, (42 USC 7384 and 20 CFR 30.701). While you are not required to respond, this information is required to obtain reimbursement for travel expenses. The method of collecting information complies with the Freedom of Information Act, the Privacy Act of 1974 and OMB Circ. 108. This form should be used for medically related travel covered by the Federal Employees' Compensation Act, the Black Lung Benefits Act and the Energy Employees Occupational Illness Compensation Program Act of 2000."

  Health Insurance Claim form OWCP 1500 OMB No. 1240-0044
  "PATIENT'S OR AUTHORIZED PERSON'S SIGNATURE I authorize the release of any medical or other information necessary to process this claim. I also request payment of government benefits either to myself or to the party who accepts assignment below."

  Patients may refuse to sign the form if they do not wish their health care providers to share their medical information.

- Privacy Impact Analysis

  Specific notice of the need to have and use privacy data to process a claim is included on the claim form itself to ensure that all claimants are aware of the data necessary to complete their claim and its uses. In addition, System of Records Notices (SORNs) which outline the users of privacy data for this system are available to the public through the DOL internet. (See list of SORNs in the External Sharing and Disclosure Section)

1.8. ACCESS, REDRESS, AND CORRECTION

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

- What are the procedures that allow individuals to gain access to their information?

  Claimants have the right to request a copy of their file at any time. They also can view their claim information via the CQS component. This is currently accessible via Employee Express, and will be available through the Department of Agriculture's National Finance Center payroll site shortly. In addition, injured workers and their representatives may access information regarding case status and compensation payments through the agency's IVR.

- What are the procedures for correcting inaccurate or erroneous information?

  Claimants can contact the closest OWCP-DFEC office and provide amended information. They are also periodically contacted by DFEC claims administrators to request updated information for their claim.

- How are individuals notified of the procedures for correcting their information?

  At the time they file the claim they are informed that they should contact the office should there be any changes in the information provided. DFEC is also in regular communication with the claimant providing the opportunity for correction of information throughout the life of the claim

- If no formal redress is provided, what alternatives are available to the individual?

  Individuals have access, redress, and amendment rights under the Privacy Act for their records, and the procedures pertaining thereto are documented in the SORN.

- Privacy Impact Analysis

  Electronic access to the claimant's records is strictly limited to preserve the privacy of the claimant. Only the claimant and/or "party in interest" (under federal regulations (20 CFR 702.113-114), any "party in interest", including the employer, the carrier, the claimant, and any lien claimant, as well as their legal representatives, have the right to a copy of the admin claim file) can request copies of their records to avoid any potential breach of privacy. Authentication is required for electronic access through AQS/CQS, ECOMP, and the IVR system.

1.9. TECHNICAL ACCESS AND SECURITY

The following questions are intended to describe technical safeguards and security measures.

- What procedures are in place to determine which users may access the system and are they documented?

  DFEC has put in place access control measures that include documented user access authorization, encryption and least privilege.

- Will Department contractors have access to the system?

  Yes.

- Describe what privacy training is provided to users, either generally or specifically relevant to the program or system?

  Annual Information System Security and Privacy Awareness Training which has a privacy module or component to it.

- What auditing measures and technical safeguards are in place to prevent misuse of data?

  OWCP uses the concept of least privilege as described above. Access is granted only after authorization based on documented access request policies. Logs for certain system functions are also reviewed on a regular basis to check for any misuse or other issues.

  All OWCP operations are required to have security audits and assessments conducted of their operations on an annual basis. All OWCP systems must have system level auditing enabled to provide for reasonable response in the event of a security situation. IT system auditing and security testing are essential aspects of how the Agency ensures the integrity and availability of our computing systems. Auditing and assessments also provide the Agency the ability to be more effective in preventing security vulnerabilities.

- Privacy Impact Analysis

  There are many potential risks when medical information is recorded about an individual, such as identity theft, certain types of insurance coverage being refused if certain medical information became public, loss of employment, etc. DFEC understands its obligation to safeguard this information to prevent any of the potential risks from being realized. Throughout this document, examples of those safeguards have been explained to illustrate this commitment to prevention of PII being compromised.

There are appropriate administrative, technical and physical safeguards in place to ensure the security and confidentiality of the information.

1.10. TECHNOLOGY

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics, and other technology.

- What stage of development is the system in, and what project development life cycle was used?

  Operations and Maintenance.

  The DOL System Development Life Cycle Management (SDLCM) Manual.

- Does the project employ technology which may raise privacy concerns? If so please discuss their implementation?

  iFECS allows limited access via its on-line web portal (CQS) to claimants to allow them to review their own information. It also allows on-line access to various other agencies' personnel who handle the compensation claims for that particular agency (AQS and ECOMP). User authentication is required to connect to both the web-portals and users are limited to those records that pertain to their own claim(s). There is also an IVR system that is available to claimants to assist them with their claims and to determine claim status. The IVR system also requires authentication of callers before any information of a sensitive (PII) nature is discussed.

  iFECS also uses the concept of least privilege to ensure that users are given access only to the information that they are required to have access to for performance of their jobs. Logging of transactions and access is also done and those logs are periodically reviewed to determine if attempts have been made to access data from either an outside source or an unauthorized user.

1.11. DETERMINATION

As a result of performing the PIA, what choices has the agency made regarding the information technology system and collection of information?

OWCP has completed the PIA for iFECS which is currently in operation. OWCP has determined that the safeguards and controls for this moderate system adequately protect the information.

OWCP has determined that it is collecting the minimum necessary information for the proper performance of a documented agency function.

1.12. PIA SIGNATURE PAGE

Douglas C Fitzgerald
Signature of Assessor
(e.g., System Owner, Operator, Developer)

6/22/12
Date

Doug Fitzgerald
Print Name

Director, DFEC
Title/Position

Paul Beckham
Signature of Program Manager (if not Assessor)

6-21-12
Date

Paul Beckham
Print Name

iFECS Project Manager, DFEC
Title/Position

OWCP/DFEC
Agency and Office/Department

200 Constitution Ave., NW
Street Address

Washington, DC 20210
City, State, and Zip Code

(202) 343-5518
Phone Number

Appendix A: Definition for PII and PII Elements

Non-Sensitive PII. PII whose disclosure cannot reasonably be expected to result in personal harm. Examples include first/last name; e-mail address; business address; business telephone; and general education credentials that are not linked to or associated with any protected PII.

Protected PII. PII whose disclosure could result in harm to the individual whose name or identity is linked to that information. Examples include, but are not limited to, social security number; credit card number; bank account number; residential address; residential or personal telephone; biometric identifier (image, fingerprint, iris, etc.); date of birth; place of birth; mother's maiden name; criminal records; medical records; and financial records. The conjunction of one data element with one or more additional elements, increases the level of sensitivity and/or propensity to cause harm in the event of compromise.

What information about individuals will be collected, generated, shared, and/or retained? Also, note whether the collection is for ☒ Federal employees, ☒ Contractor staff, or ☒ Members of the Public. {Check all that apply}

- ☒ First and/or last name
- ☒ Date of birth
- ☐ Place of birth
- ☐ Mother's maiden name
- ☒ SSN
- ☐ SSN {truncated)
- ☒ SSN (elongated)
- ☐ Military, immigration, or other government-issued identifier
- ☐ Photographic identifiers (i.e., photograph image, x-rays, video)
- ☐ Biometric identifier (i.e., fingerprint, voiceprint, iris)
- ☐ Other physical identifying information (e.g., tattoo, birthmark)
- ☐ Vehicle identifier (e.g., license place, VIN)
- ☐ Driver's license number
- ☒ Residential address
- ☒ Personal phone numbers (e.g., phone, fax, cell)
- ☒ Mailing address (e.g., P.O. Box)
- ☐ Personal e-mail address

☒ Business address

☒ Business phone number (e.g., phone, fax, cell)

☐ Business e-mail address

☒ Medical information including physician's notes

☒ Medical record number

☐ Device identifiers (e.g., pacemaker, hearing aid)

☐ Employer Identification Number (EIN)/Taxpayer Identification Number (TIN)

☒ Financial account information and/or number (e.g., checking account number, PIN, retirement, investment account)

☒ Certificates (e.g., birth, death, marriage)

☒ Legal documents or notes (e.g., divorce decree, criminal records)

☐ Educational records

☐ Network logon credentials (e.g., username and password, public key certificate)

☐ Digital signing or encryption certificate

☒ Other: Employment Records

☒ Other: Survivor Eligibility Data, (e.g., relationship, marriage, divorce, death)

☒ Other: Wage/Salary Information

☒ Other: Government Benefits data