ADAMS ML19198A288

U.S. Nuclear Regulatory Commission

Privacy Impact Assessment

Designed to collect the information necessary to make relevant determinations regarding the applicability of the Privacy Act, the Paperwork Reduction Act information collection requirements, and records management requirements.

Employee Compensation Operation and Management Portal (ECOMP)

Date: July 17, 2019

A. GENERAL SYSTEM INFORMATION

1. Provide a detailed description of the system:

The Office of Workers Compensation Programs (OWCP) - Department of Labor (DOL) completed a comprehensive update of the Federal Employee Compensation Act (FECA) regulations in 20 C.F.R. Part 10, effective August 29, 2011. 20 CFR §§ 10.100, 10.101,10.102 and 10.103 (Claims for traumatic injury, occupational disease, wage loss compensation, and schedule awards respectively) direct that all such notices should be submitted electronically wherever feasible to facilitate processing of such claims. Each of these regulations also explicitly requires that, "All employers that currently do not have such capability should create such a method by December 31, 2012."

To facilitate electronic form filing, the OWCP has created its own web-based application called Employees Compensation and Management Portal (ECOMP), with a comprehensive electronic system for recording workplace injuries and illnesses, and processing claims under the FECA. ECOMP is available to all federal agencies who wish to use it for electronic form filing free of charge.

ECOMP, which was released to the public on November 2, 2011, can be accessed directly at the following url: https://www.ecomp.dol.gov. The site currently contains two different types of functionality – electronic submission of documents and electronic submission of FECA claim forms.

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 subcomponents, 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 Nuclear Regulatory Commission (NRC) will only use the eCOMP system to manage federal workers compensation claims.

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.

2. What agency function does it support?

Executive Order 12193 – Occupational Safety and Health Programs for Federal Employees (1980) Empowers OSHA to inspect and cite Federal agencies for safety violations. Supervisors must ensure that facilities are safe and can pass OSHA inspections.

Federal Regulation 29 CFR 1960 – Elements for Federal OSH Programs established basic safety program elements Federal agencies must follow:
- Employees are covered by OSHA no matter where work takes them even abroad
- Employees must be removed from unsafe private sector facilities
- Employees are safe from reprisal
- Safety training is mandatory

Federal Regulation 29 CFR 1904 – Recording and Reporting Occupational Injuries and Illnesses:
- Each agency shall maintain a log of all occupational injuries and illnesses for each establishment.
- Within 6 working days after receiving information on an occupational injury/illness, appropriate information concerning such injury shall be entered on the log
- You must post a copy of the annual summary in each establishment in a conspicuous place where notices to employees are customarily posted.

This system will support NRC Safety and Health Occupational Programs:
- OSHA Compliance

- *Workplace Hazard Assessments*
- *Written Safety Policy*
- *Specific OSHA Programs*
- *Investigation of Serious Accidents*
- *Medical Surveillance Services*

3. Describe any modules or subsystems, where relevant, and their functions.

The eCOMP system feature enables all stakeholders to upload documents directly into a FECA case file. Stakeholders include, but are not limited to, injured workers (and their representatives), employing agencies, contract field nurses and rehabilitation counselors, and medical providers. Many of the letters used by the Division of Federal Employees' Compensation (DFEC) contain language referencing this option for document submission.

A user does not have to register or enroll with eCOMP to use this feature. Rather, any stakeholder with an internet connection and specific information about a FECA claim can upload documents directly into the case file. Before attempting to upload documents via ECOMP, a user needs to have the following pieces of information: claim number, claimant's last name, claimant's date of birth, and the date of injury. If these pieces of information do not match the OWCP case data exactly, submission of a document is not allowed.

Once a document has been uploaded to the case file, ECOMP can only be used to verify that the OWCP received the document, not when or if a response has been provided. Any stakeholder having a question about a document that has been submitted must contact the servicing District Office.

Some specific documents should NOT be uploaded through the WEEDS component of ECOMP. The ECOMP interface and associated documentation clearly note these exceptions, which include the following:

a) CA-1 (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)

These forms should all be sent to DFEC's Consolidated Case Create Facility (US Department of Labor, OWCP/DFEC, 400 West Bay Street, Room 827, Jacksonville, FL 32202), if not electronically filed through ECOMP (see next section) or other approved electronic forms submission platforms.

b) CA-16 (Authorization for Examination and/or Treatment)
CA-2a (Notice of Recurrence)
CA-5 (Claim for Compensation by Widow, Widower, and/or Children)

These forms should be sent to the DFEC Consolidated Case Create Facility.

c) OWCP-915 (Claim for Medical Reimbursement)
OWCP-957 (Medical Travel Refund Request)

These forms should be submitted to the DFEC's central mailroom (US Department of Labor, OWCP/DFEC, PO Box 8300, London, KY 40742-8300).

d) Medical bills and requests for authorization of medical procedures from medical providers

These should be submitted through the OWCP's Central Billing and Authorization Facility (see the DFEC website for more information).

e) Appellate requests for the Branch of Hearings and Review and the Employees' Compensation Appeals Board

Each should be sent to the specific address outlined in the appeal rights that accompany any formal decision.

4. What legal authority authorizes the purchase or development of this system?

The Department of Labor (DOL) administers and enforces more than 180 federal laws. These mandates and the regulations that implement them cover many workplace activities for about 10 million employers and 125 million workers.

*The **Federal Employees' Compensation Act (FECA)**, 5 U.S.C. 8101 et seq., establishes a comprehensive and exclusive workers' compensation program which pays compensation for the disability or death of a federal employee resulting from personal injury sustained while in the performance of duty. The FECA, administered by OWCP, provides benefits for wage loss compensation for total or partial disability, schedule awards for permanent loss or loss of use of specified members of the body, related medical costs, and vocational rehabilitation.*

*The **Longshore and Harbor Workers' Compensation Act (LHWCA)**, administered by The **Office of Workers Compensation Programs (OWCP),** provides for compensation and medical care to certain maritime employees (including a longshore worker or other person in longshore operations, and any harbor worker, including a ship repairer, shipbuilder, and shipbreaker) and to*

qualified dependent survivors of such employees who are disabled or die due to injuries that occur on the navigable waters of the United States, or in adjoining areas customarily used in loading, unloading, repairing or building a vessel.

*The **Energy Employees Occupational Illness Compensation Program Act (EEOICPA)** is a compensation program that provides a lump-sum payment of $150,000 and prospective medical benefits to employees (or certain of their survivors) of the Department of Energy and its contractors and subcontractors as a result of cancer caused by exposure to radiation, or certain illnesses caused by exposure to beryllium or silica incurred in the performance of duty, as well as for payment of a lump-sum of $50,000 and prospective medical benefits to individuals (or certain of their survivors) determined by the Department of Justice to be eligible for compensation as uranium workers under section 5 of the **Radiation Exposure Compensation Act (RECA)**.*

*The **Black Lung Benefits Act (BLBA)** provides monthly cash payments and medical benefits to coal miners totally disabled from pneumoconiosis ("black lung disease") arising from their employment in the nation's coal mines. The statute also provides monthly benefits to a deceased miner's survivors if the miner's death was due to black lung disease.*

***STATUTORY AND REGULATORY PROVISIONS:** FECA claim file information is covered by the Privacy Act of 1974. See 5 U.S.C. 552a. The FECA regulations at 20 C.F.R. §10.11 provide in part that "All records relating to claims for benefits filed under the FECA, including any copies of such records maintained by an employing agency, are covered by the government-wide Privacy Act system of records entitled DOL/GOVT-1 (Office of Workers' Compensation Programs, Federal Employees' Compensation Act File). This system of records is maintained by and under the control of the OWCP, and, as such, all records covered by DOL/GOVT-1 are official records of the OWCP." DOL/GOVT-1 provides that federal agencies that employed the claimant at the time of the occurrence or recurrence of the injury or occupational illness can access OWCP case file information in order to verify billing, to assist in administering the FECA, to answer questions about the status of the claim, to consider rehire, retention or other actions the agency may be required to take with regard to the claim, or to permit the agency to evaluate its safety and health program. 77 Fed. Reg. 1728, at 1738-41 (January 11, 2012), viewable at http://www.gpo.gov/fdsys/pkg/FR-2012-01-11/pdf/2012-345.pdf.*

5. What is the purpose of the system and the data to be collected?

ECOMP was released to the public on November 2, 2011 and can be accessed directly at the following url: https://www.ecomp.dol.gov. The site originally

contained two different types of functionality – electronic submission of documents and electronic submission of Federal Employees' Compensation Act (FECA) claim forms. See FECA Circular 13-03, Employees' Compensation and Management Portal (ECOMP), for more detail on those features.

Effective April 9, 2013, ECOMP was enhanced to create a third functionality to allow designated ECOMP Agency Reviewers (AR) the ability to view imaged documents for cases assigned to their agency. The new functionality is called Agency Reviewer Imaging (ARi). Initially, only a few specific agencies were granted such access; however, after this initial deployment phase, ARi access will be provided to other enrolled agencies on a rolling basis.

Employing Agencies can currently review/obtain case file documents, but must do so by other means, such as submitting a written request to the OWCP or by visiting the district office and reviewing/printing documents on a kiosk. Deployment of ARi allows the OWCP and Employing Agencies to contain costs and increase program efficiencies by providing ARs access to the case documents without generation and submission of a written request or scheduling a visit with the district office, and by eliminating the time and expense it takes the OWCP to respond to such requests. Allowing the ARs to view case file documents also facilitates better Employing Agency collaboration with the OWCP in regard to disability management and return-to-work efforts. For example, the Employing Agency can view work restrictions in a case and craft a job offer for the injured worker without first making a request to the OWCP for such medical evidence and waiting for the OWCP's response. This allows the injured workers to return to work as soon as possible, which furthers the OWCP's mission to facilitate reemployment of injured workers who are able to work.

ACTIONS:

A. Intended Use

1. Each time an AR accesses a case, he/she receives a Privacy Act warning consistent with DOL/GOVT-1, which is referenced above:

Access to this case file and data must be restricted to only those authorized employees who need it to perform their official duties, and confidentiality of the records should be protected in such a way that unauthorized persons do not have access to any such records.

Case documentation and data contained in this system is and remains Department of Labor data that is subject to the Privacy Act (5 U.S.C. 552a) and to the Systems Notice for DOL/GOVT-1. Absent a court order from a court of competent jurisdiction or a written release from the individual FECA claimant, such data may only be used pursuant to DOL's OWCP interpretation of a routine use published in DOL/GOVT-1 and in a manner that is compatible with the

purpose for which the record was created; that purpose is the administration and payment of FECA compensation. Before any data from DOL/GOVT-1 can be used in a personnel or similar action, there must be a written release from the claimant or an order from a court of competent jurisdiction, or agreement by DFEC management that disclosure of the information is permitted under the Privacy Act. For further information see http://www.dol.gov/sol/privacy/dol-govt-1.htm.

2. By proceeding with the retrieval of the case after having received such warning, the AR is certifying that he/she is accessing the case file information for a reason consistent with a published routine use.

B. Access

1. ARi is a feature granted only to agencies that have executed a Memorandum of Understanding (MOU) with the OWCP relative to ECOMP (see FECA Circular 13-03), and are actively using ECOMP to electronically file workers' compensation forms (CA-1/2s and/or CA-7s).

2. ARi functionality is limited to users granted access to a Digital Rights Management (DRM) license. A specific number of licenses is provided to agencies actively using ECOMP for forms filing.

3. DRM licenses are granted to an agency's ECOMP Agency Maintenance User (AMU) by the ECOMP DFEC Administrator. These licenses are then assigned to specific AR users under that AMU's jurisdiction. When providing ARi access to an AR, the AMU is required to instruct each user that only that single user may utilize his/her license in accordance with this guidance. The DFEC Administrator and the AMU can verify who has access to ARi for a specific agency at any time via a specific application in ECOMP.

4. The assignment of a DRM license activates the ARi feature enabling designated ARs to view imaged workers compensation cases assigned to chargeback codes to which that AR is already assigned.

C. Reviewing Cases

1. The ARi user must have the following pieces of information: claim number, claimant's last name, claimant's date of birth, and the date of injury. If these pieces of information do not match the OWCP case data exactly, or if the case is not assigned to a chargeback code to which the AR has been granted access in ECOMP, viewing of the requested case will not be permitted.

2. ARi users may download up to 5 cases to their Review Cases Dashboard. It takes approximately 24 hours from the time the request is made to the time the imaged case becomes available to the ARi user.

3. Cases may be viewed for up to 5 calendar days, but an ARi user may release a case at any time to free-up a slot on the Dashboard. The user can only see documents available at the time the case is requested; there is no refresh option.

4. ARi users can view all imaged documents in a case that have been received within the last 3 years, as well as all other imaged documents beyond 3 years old that are indexed in the OWCP case file as a decision, a form, or as outgoing correspondence.

D. Saving and Printing Documents

1. ARi users may download/save any or all documents in a case on their dashboard.

2. When the user chooses to download a document, he/she must first indicate why the documents are being saved. An available list of the "routine uses" is provided, but there is no default. The ARi user must choose an available option before ECOMP will download the documents. Available choices are:
- To answer questions about the status of the claim
- To consider return-to-work opportunities
- To evaluate the agency's safety and health program
- To assess continuing eligibility for FECA benefits
- To verify billing

3. Documents are downloaded via a secure PDF document. This PDF document is encrypted using DRM and is accessible only to the ARi user who created the document.

4. Each time the secure PDF document is accessed, the ARi user is required to enter his/her ECOMP user ID and password. If the user ID and password for the document are not valid, the user will not be granted access to that document.

5. Each page of every document downloaded from ECOMP by an ARi user will be marked with an annotation atop the document that indicates it was "Printed from ECOMP," with the user's ECOMP user ID and the date it was printed.

E. Documentation of Case File Review and Record of Saved/Printed Documents

1. The fact that a case was reviewed in ARi is recorded in the OWCP case file via an automated memo uploaded directly to the case by the ECOMP system. This memo denotes when a case was accessed and who accessed it.

2. The memo for the OWCP case file also details any documents that the Ari user saved/printed and the reason for such action. See D2 above.

6. Points of Contact:

Project Manager	**Office/Division/Branch**	**Telephone**
Rick Grancorvitz	OCHCO/HCAB	301-287-0805
Business Project Manager	**Office/Division/Branch**	**Telephone**
Susan Salter	OCHCO/ADHROP/OB	301-287-0545
Technical Project Manager	**Office/Division/Branch**	**Telephone**
Brendan Cain	OCHCO/HCAB	301-287-0552
Executive Sponsor	**Office/Division/Branch**	**Telephone**
Jason Shay	OCHCO/ADHROP	301-287-0590
ISSO	**Office/Division/Branch**	**Telephone**
Brendan Cain	OCHCO/HCAB	301-287-0805
System Owner/User	**Office/Division/Branch**	**Telephone**
Susan Salter	OCHCO/ADHROP/OB	301-287-0545

7. Does this privacy impact assessment (PIA) support a proposed new system or a proposed modification to an existing system?

a. ____ New System

____ Modify Existing System

__X__ Other

This PIA supports an existing system called eCOMP that has been developed and will be maintained by the Department of Labor. NRC use of the system will be free to all users in the agency

b. If modifying or making other updates to an existing system, has a PIA been prepared before?

Not Applicable

(1) If yes, provide the date approved and ADAMS accession number.

(2) If yes, provide a summary of modifications or other changes to the existing system.

8. Do you have an NRC system Enterprise Architecture (EA)/Inventory number?

Yes

a. If yes, please provide Enterprise Architecture (EA)/Inventory number.

20170004

b. If, no, please contact EA Service Desk to get Enterprise Architecture (EA)/Inventory number.

B. INFORMATION COLLECTED AND MAINTAINED

These questions are intended to define the scope of the information requested as well as the reasons for its collection. Section 1 should be completed only if information is being collected about individuals. Section 2 should be completed for information being collected that is not about individuals.

1. INFORMATION ABOUT INDIVIDUALS

a. Does this system maintain information about individuals?

Yes

(1) If yes, identify the group(s) of individuals (e.g., Federal employees, Federal contractors, licensees, general public (provide description for general public (non-licensee workers, applicants before they are licenses etc.)).

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.

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, 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.

(2) IF NO, SKIP TO QUESTION B.2.

b. What information is being maintained in the system about an individual (**be specific** – e.g. SSN, Place of Birth, Name, Address)?

- 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

c. Is information being collected from the subject individual?

To the greatest extent possible, collect information about an individual directly from the individual.

Yes

(1) If yes, what information is being collected?

The FECA benefit process is initiated when a claimant (federal employee or dependent) submits a notice of injury, occupational disease, or death 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.

d. Will the information be collected from individuals who are not Federal employees?

Yes

(1) If yes, does the information collection have OMB approval?

Yes

(a) If yes, indicate the OMB approval number:

- 1240-0007, Form OWCP-915
- 1240-0009, Form CA-2a
- 1240-0013, Form CA-5 and CA-5B
- 1240-0037, Form OWCP-957
- 1240-0046, Forms CA-7, CA-16, and CA-20

e. Is the information being collected from existing NRC files, databases, or systems?

No

(1) If yes, identify the files/databases/systems and the information being collected.

f. Is the information being collected from external sources (any source outside of the NRC)?

Yes

(1) If yes, identify the source and what type of information is being collected?

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.

g. How will information not collected directly from the subject individual be verified as current, accurate, and complete?

For Electronic Data Interchange (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.

Claimants can correct inaccurate or erroneous information by contacting 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.

Individuals are notified at the time they file the claim 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.

h. How will the information be collected (e.g. form, data transfer)?

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.

2. **INFORMATION NOT ABOUT INDIVIDUALS**

a. Will information not about individuals be maintained in this system?

No

(1) If yes, identify the type of information (be specific).

b. **What is the source of this information? Will it come from internal agency sources and/or external sources? Explain in detail.**

C. USES OF SYSTEM AND INFORMATION

These questions will identify the use of the information and the accuracy of the data being used.

1. Describe all uses made of the data in this system.

The system permits claimants, representatives, employing agency staff and medical providers to upload documents directly into existing OWCP files through the internet. ECOMP enables Claims Examiners (CEs) to view the new information within four hours of submission.

Registration is not required to upload documents. Claimants need only provide a case number, their last name, date of birth and the date of injury to access the user-friendly system. As an added security measure, these four identifiers must precisely match the existing file information. Users who experience difficulty accessing a claim will have to contact the respective OWCP District Office (DO) to acquire the necessary data.

Multiple documents submitted through ECOMP must be uploaded individually, never as a combined document. Users will need to categorize each document as Medical or Incoming. The Nurse and Rehab categories are reserved for nurses and rehabilitation counselors working for OWCP's Nurse Intervention or Vocational Rehabilitation programs. The Medical category is used for all medical documentation such as test results, narratives, physician notes, forms CA-20 and OWCP 5, work tolerance limitations and functional capacity evaluations.

The Incoming category should be selected for documents that do not fit the other three more specific categories, such as job offers, elections of benefits or even witness statements. The Incoming category can also be used to pose questions to CEs; responses, however, will be provided by mail.

Users will not be penalized for misidentifying documentation. When the upload process is finished, a Document Control Number (DCN) will be issued as proof of

submission and for tracking purposes. To obtain any additional information pertaining to document disposition, the designated DO must be contacted. CEs will not need the DCN to locate documents.

2. Is the use of the data both relevant and necessary for the purpose for which the system is designed?

Yes

3. Who will ensure the proper use of the data in this system?

OWCP uses the concept of least privilege. 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.

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.

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

4. Are the data elements described in detail and documented?

Yes

a. If yes, what is the name of the document that contains this information and where is it located?

OWCP — Integrated Federal Employees' Compensation System (iFECS)
— FY 2013 Overview
http://www.dol.gov/oasam/ocio/programs/PIA/OWCP/OWCP-iFECS.htm

5. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

No

Derived data is obtained from a source for one purpose and then the original information is used to deduce/infer a separate and distinct bit of information that is aggregated to form information that is usually different from the source information.

Aggregation of data is the taking of various data elements and then turning it into a composite of all the data to form another type of data (i.e. tables or data arrays).

a. If yes, how will aggregated data be maintained, filed, and utilized?

b. How will aggregated data be validated for relevance and accuracy?

c. If data are consolidated, what *controls* protect it from unauthorized access, use, or modification?

6. How will data be *retrieved* from the system? Will data be retrieved by an individual's name or personal identifier (name, unique number or symbol)? (Be specific.)

Data will be retrieved by an individual's Case Number, Name or Social Security Number (SSN).

a. If yes, explain, and list the identifiers that will be used to retrieve information on the individual.

7. Has a Privacy Act System of Records Notice (SORN) been published in the Federal Register?

Yes

a. If "Yes," provide name of SORN and location in the Federal Register.

General Personnel Records (Official Personnel Folder and Related Records) - 11

8. If the information system is being modified, will the SORN(s) require amendment or revision?

9. Will this system provide the capability to identify, locate, and monitor (e.g., track, observe) individuals?

Yes

a. If yes, explain.

(1) What controls will be used to prevent unauthorized monitoring?

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.

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.

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.

10. List the report(s) that will be produced from this system.

Reports of injury by the employee and/or employing agency; Medical records and reports information relating to vocational and/or medical rehabilitation plans and progress reports;

a. What are the reports used for?

DFEC receives reports or documents from its Customs and Border Protections (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.

b. Who has access to these reports?

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.

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.

D. ACCESS TO DATA

1. Which NRC office(s) will have access to the data in the system?

Office of the Chief Human Capital Office (OCHCO), Workforce Management and Benefits Branch (WMHB) Human Resource Specialists.

(1) For what purpose?

To review and approve NRC employees claims for compensation cases.

(2) Will access be limited?

Access will be limited to specific NRC employees who have been given authority to access, review and approve NRC employee claims for compensation cases.

2. Will other NRC systems share data with or have access to the data in the system?

No

(1) If yes, identify the system(s).

(2) How will the data be transmitted or disclosed?

3. Will external agencies/organizations/public have access to the data in the system?

Yes

(1) If yes, who?

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.

(2) Will access be limited?

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.

(3) What data will be accessible and for what purpose/use?

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.

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.

(4) How will the data be transmitted or disclosed?

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.

E. RECORDS AND INFORMATION MANAGEMENT (RIM) - RETENTION AND DISPOSAL

The National Archives and Records Administration (NARA), in collaboration with federal agencies, approves whether records are temporary (eligible at some point for destruction/deletion because they no longer have business value) or permanent (eligible

at some point to be transferred to the National Archives because of historical or evidential significance). These determinations are made through records retention schedules and NARA statutes (44 U.S.C., 36 CFR). Under 36 CFR 1234.10, agencies are required to establish procedures for addressing records management requirements, including recordkeeping requirements and disposition, before approving new electronic information systems or enhancements to existing systems. The following question is intended to determine whether the records and data/information in the system have approved records retention schedule and disposition instructions, whether the system incorporates Records and Information Management (RIM) and NARA's Universal Electronic Records Management (ERM) requirements, and if a strategy is needed to ensure compliance.

1) Can you map this system to an applicable retention schedule in NRC's Comprehensive Records Disposition Schedule(NUREG-0910), or NARA's General Records Schedules?

Yes

a. If yes, please cite the schedule number, approved disposition, and describe how this is accomplished (then move to F.1).

100	**Workers' Compensation (personnel injury compensation) records.** Federal Employees' Compensation Act case files on injuries Federal employees sustain, while performing their duties that result in lost time or death, whether or not the employee filed a workers' compensation claim. Includes: • forms, reports, correspondence, claims • medical and investigatory records • administrative determinations or court rulings • payment records	**Records of agencies that forward case file material to DOL for retention in DOL's master OWCP records.**	**Temporary.** Destroy 3 years after compensation ceases or when deadline for filing a claim has passed.
101		**Records of agencies that do not forward case file material to DOL for retention in DOL's master OWCP**	**Temporary.** Destroy 15 years after compensation ceases or when deadline for filing a claim has passed.

	Exclusion 1: Copies filed in the Employee Medical Folder. **Exclusion 2:** Records created and maintained by the Department of Labor's Office of Workers' Compensation.	**records.**	

b. If no, please contact the Records and Information Management (RIM) staff at ITIMPolicy.Resource@nrc.gov.

F. TECHNICAL ACCESS AND SECURITY

1. Describe the security controls used to limit access to the system (e.g., passwords).

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

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.

2. What controls will prevent the misuse (e.g., unauthorized browsing) of system data by those having access?

OWCP uses the concept of least privilege. 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.

3. Are the criteria, procedures, controls, and responsibilities regarding access to the system documented?

Yes

(1) If yes, where?

Criteria, procedures, controls, and responsibilities regarding access to the system is documented and located on the eCOMP web portalhttps://www.ecomp.dol.gov/. Once a federal agency has completed the necessary documents to be approved to use the system, their employees can be allowed to gain access to use the system.

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.

4. Will the system be accessed or operated at more than one location (site)?

No

a. If yes, how will consistent use be maintained at all sites?

5. Which user groups (e.g., system administrators, project managers, etc.) have access to the system?

Agency Maintenance User – ECOMP Power User at the Agency
Agency Reviewer– Injury Compensation Specialist at the Agency

OSHA Record Keeper – Safety staff at the Agency responsible for OSHA reporting
Employee– Manages own account and registration
Supervisor – No account needed
Auditor - Manages proper use of the system

6. Will a record of their access to the system be captured?

Yes

a. If yes, what will be collected?

User id, date and action performed.

7. Will contractors be involved with the design, development, or maintenance of the system?

Yes

If yes, and if this system will maintain information about individuals, ensure Privacy Act and/or PII contract clauses are inserted in their contracts.

- *FAR clause 52.224-1 and FAR clause 52.224-2 should be referenced in all contracts, when the design, development, or operation of a system of records on individuals is required to accomplish an agency function.*
- *PII clause, "Contractor Responsibility for Protecting Personally Identifiable Information" (June 2009), in all contracts, purchase orders, and orders against other agency contracts and interagency agreements that involve contractor access to NRC owned or controlled PII.*

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

OWCP uses the concept of least privilege. 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.

9. Is the data secured in accordance with FISMA requirements?

Yes

a. If yes, when was Certification and Accreditation last completed?

TBD

PRIVACY IMPACT ASSESSMENT REVIEW/APPROVAL
(For Use by OCIO/GEMS/ISB Staff)

System Name: Employee Compensation Operation and Management Portal (ECOMP)

Submitting Office: Office of the Chief Human Capital Officer

A. PRIVACY ACT APPLICABILITY REVIEW

____ Privacy Act is not applicable.

_X_ Privacy Act is applicable.

Comments:
Personally identifiable information will be maintained by eCOMP. NRC's collection and use of this information is covered by the following NRC Privacy Act system of records: NRC-11, General Personnel Records (Official Personnel Folder and Related Records). The NRC will only use the eCOMP system to manage federal workers compensation claims.

Reviewer's Name	Title	Date
Sally A. Hardy	Privacy Officer	9/18/2019

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION

____ No OMB clearance is needed.

_X_ OMB clearance is needed.

____ Currently has OMB Clearance. Clearance No._____

Comments:
The Department of Labor Clearances are listed in the PIA.

Reviewer's Name	Title	Date
David Cullison	Agency Clearance Officer	8/12/19

C. RECORDS RETENTION AND DISPOSAL SCHEDULE DETERMINATION

___ No record schedule required.

____ Additional information is needed to complete assessment.

____ Needs to be scheduled.

__X__ Existing records retention and disposition schedule covers the system - no modifications needed.

Comments:

Reviewer's Name	Title	Date
Marna Dove	Electronic Records Manager	9/11/2019

D. BRANCH CHIEF REVIEW AND CONCURRENCE

____ This IT system **does not** collect, maintain, or disseminate information in identifiable form from or about members of the public.

__X__ This IT system **does** collect, maintain, or disseminate information in identifiable form from or about members of the public.

I concur in the Privacy Act, Information Collections, and Records Management reviews:

/RA/ Date November 29, 2019

Anna T. McGowan, Chief
Information Services Branch
Governance & Enterprise Management
Services Division
Office of the Chief Information Officer

TRANSMITTAL OF PRIVACY IMPACT ASSESSMENT/
PRIVACY IMPACT ASSESSMENT REVIEW RESULTS

TO: **Jason Shay, Office of the Chief Human Capital Officer**	
Name of System: **Employee Compensation Operation and Management Portal (ECOMP)**	
Date ISB received PIA for review: **July 17, 2019**	Date ISB completed PIA review: **September 18, 2019**
Noted Issues:	
Anna T. McGowan, Chief Information Services Branch Governance & Enterprise Management Services Division Office of the Chief Information Officer	Signature/Date: **/RA/ November 29, 2019**
Copies of this PIA will be provided to: *Thomas Ashley, Director* *IT Services Development & Operation Division Office of the Chief Information Officer* *Jonathan Feibus* *Chief Information Security Officer (CISO))* *Governance & Enterprise Management Service Division* *Office of the Chief Information Officer*	