Template Version Number: 01-2020

U.S. Department of Commerce
Office of the Secretary

Privacy Threshold Analysis

for the

OS/OOSH Workers Compensation Claims Medical Case Management System (WC-CMCMS) OS-062

U.S. Department of Commerce Privacy Threshold Analysis

OS/OOSH Workers Compensation Claims Medical Case Management System (WC-CMCMS)

Unique Project Identifier: OS-062

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

The Workers' Compensation Claims and Medical Case Management System (WC-CMCMS) through the overall Workers' Compensation Service Program (WCSP) assists the Department with medical review and oversight of all WC claims to ensure injured employees receive timely and appropriate medical care to enable a successful return to the workforce as soon as medically appropriate.

a) *Whether it is a general support system, major application, or other type of system*
The WC-CMCMS is a Major Application system in accordance with Office of Management and Budget (OMB) Circular A-130, Appendix III that provides access to WebOPUS, a secure managed web application for the Department of Commerce.

b) *System location*
The system is hosted in a FedRAMP-accredited data center operated by CGI Federal and located in Phoenix, AZ. It consists of the software, hardware, and infrastructure components necessary to run the WebOPUS application.

c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*
The system has authorized interconnections with two third-party systems: Sfax, which is a secure cloud fax service and OPTUM which provides pharmacy services.

d) The purpose that the system is designed to serve

WC-CMCMS is part of a contracted workers' compensation service, available for all DOC Bureaus. Users of the WC-CMCMS system include contractor employees and Department of Commerce (DOC) specific employees at each bureau with oversight for workers' compensation. Managed Care Advisors, as contractors to DOC, designated contract employees are permitted to review claim related clinical information under the provisions of the Federal Employees' Compensation Act (FECA) in accordance with the Privacy Act. Depending on case volume, DOC Bureau Workers' Compensation Coordinators (WCCs) have access to WC-CMCMS.

e) The way the system operates to achieve the purpose

WC-CMCMS is administered by a component Program Director who authorizes user access/ level of access to the system. WC-MCMS users are provided training on the system prior to being granted access and must sign a confidentiality or non-disclosure agreement upon entry on duty. Access to the PII/BII is restricted to authorized personnel only, whose activities are closely monitored in an MCM service database.

f) A general description of the type of information collected, maintained, used, or disseminated by the system

This information may include: social security numbers (SSN); date of birth; home address and phone number; place/date/cause/nature of injury; Employer name/address; OWCP Agency Code; claimant's work address; date notice received; supervisor name; doctor treating the work related injury; medical notes/reports pertinent to the injury; medication name/dosage/strength/prescribing provider; and salary amounts lost.

g) Identify individuals who have access to information on the system

Bureau users may only see data from their own Bureaus. There is no intra-departmental access of workers' compensation information. Only the DOC headquarters department WC office can view all Department's WC data to conduct statistical and management reports, and to ensure compliance and general oversight of the entire program. Users must have a valid need to know before they are granted access to their component (bureau) information in WC-CMCMS. The workers' compensation claims services contractor, Managed Care Advisors (MCA) and designated employees have "contactor" access. The bureau WC Program Director authorizes user access and level of access to the system. Authorized users are closely tracked and monitored for continued usage and need-to-know. Users are provided training on the system prior to being given access.

h) How information in the system is retrieved by the user

All authorized users are permitted to access the WC-CMCMS system remotely. Remote access to WC-CMCMS is provided through the use of an encrypted (https) session and multi-factor authentication (MFA). Contractors, or designated contract employees with the WC Services contractor, or Managed Care Advisors, are permitted to review claim related clinical information under the provisions of the FECA in accordance with the Privacy Act. These individuals access the system via an encrypted Citrix session. Citrix session authentication incorporates MFA via Duo Security. System, network, and data administrators performing maintenance access the system using a virtual private network (VPN) and MFA via Entrust.

i) How information is transmitted to and from the system

At the first report of injury, information is collected from the CA-1 or CA-2 claim form filed by the claimant. Information is also collected from the injured worker, treating health care providers, DOC workers' compensation professionals, and the Department of Labor (DOL). Injured workers (including former employees) submit information via DOL's Employee Compensation Operations & Maintenance Portal (ECOMP) system, which is then manually entered into WC-CMCMS by WC Claims Specialists as provided on the claim form. This is then supplemented with additional information gathered by the Medical Case Manager. This information may include name; SSN; date of birth; home address and phone number; place/date/cause/nature of injury; Employer name/address; Office of Workers' Compensation Programs (OWCP, which is under DOL) Agency Code; claimant's work address; date notice received; supervisor name; doctor treating the work-related injury; medical notes/reports pertinent to the injury; medication name/dosage/strength/prescribing provider; and salary amounts lost.

Injured workers are responsible for providing their medical evidence to DOL. The medical evidence includes information from treating health care providers such as an injury diagnosis, prognosis, treatment plan, physician name and office address, medication name, dosage, etc. Treating physicians do not have access to ECOMP or WC-CMCMS.

DOC workers' compensation professionals provide a brief summary of the normal work duties and physical requirements of the job, and which duties may safely be performed within specific physical limitations. To assist the injured employee, DOC workers' compensation professionals may also submit treating physician information; medical notes/reports; medication information; OWCP Agency Code; and fills in any gaps in needed information above.

The DOL/OWCP creates a claim number when a claim is filed in ECOMP. Case status information and supporting documentation is available to the employing agency (DOC) via DOL's Agency Query System (AQS), which is an agency portal into ECOMP information. Information may be collected from any of these sources via verbal communications or written communications sent via paper mail or secure e-fax. In addition, DOC may receive

information from DOL/OWCP via the AQS (an online password-protected site owned, operated, and managed by DOL/OWCP), the DOL/OWCP online billing web-portal, on-site review of the official claims record, or via the DOL/OWCP ECOMP. Neither AQS nor ECOMP have direct connections to the WC-CMCMS. DOC workers' compensation professionals have direct log-in access to AQS so they can query a case status in ECOMP and any other submitted documentation. WC specialist maintains an email address, if needed for claimants to submit information. However, WC specialist recommends not sending medical documentation or information with PII over email.

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or 01-2017). *Continue to answer questions and complete certification.*

__X__ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2019 or later). *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

____ Yes. This is a new information system.

____ Yes. This is an existing information system for which an amended contract is needed.

____ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

__X__ No. This is not a new information system.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

__X__ No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

____ Yes, the IT system collects, maintains, or disseminates BII.

__X__ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

__X__ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

_X__ DOC employees
____ Contractors working on behalf of DOC
____ Other Federal Government personnel
____ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

_X__ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form. SSN is needed to allow DOC workers' compensation staff direct login access to AQS (online password protected DOL/OWCP managed website) to query a case status in Department of Labor's Employee Compensation Operations & Maintenance Portal (ECOMP). All data is retained only to support the time necessary to fully close a claim. Social Security number is collected and maintained by DOL and is needed by DOC to differentiate between claims in DOL's systems. SSN is also used to verify claim forms filed by DOC claimants, which require SSN per DOL.
Provide the legal authority which permits the collection of SSNs, including truncated form. 5 U.S.C. § 8145 gives DOL/OWCP the sole authority to manage all federal employee injury claims. DOC, as an "employing agency" under the FECA, has the authority "to carry out the functions vested in the employer under the FECA, including officers or employees delegated responsibility by an employer for authorizing medical treatment for injured employees."(20 CFR 10.5)

____ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

__X__ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

_X__ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

____ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

☑ I certify the criteria implied by one or more of the questions above **apply** to the WC-CMCMS and as a consequence of this applicability, I will perform and document a PIA for this IT system.

☐ I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer or System Owner Name: Stewart Merritts Office: Office of Occupational Safety and Health Phone: 202-482-3243 Email: smerritts@doc.gov Signature: STEWART MERRITTS Digitally signed by STEWART MERRITTS Date: 2021.07.28 11:13:27 -04'00' Date signed:	**Information Technology Security Officer** Name: Jerome Nash Office: US Department of Commerce Phone: 202-482-5929 Email: Jnash@doc.gov Signature: JEROME NASH Digitally signed by JEROME NASH Date: 2021.07.28 11:44:48 -04'00' Date signed:
Privacy Act Officer Name: Tahira Murphy Office: Office of Privacy and Open Government Phone: 202-482-8075 Email: TMurphy2@doc.gov Signature: TAHIRA MURPHY Digitally signed by TAHIRA MURPHY Date: 2021.09.13 12:25:46 -04'00' Date signed:	**Authorizing Official** Name: Lawrence W. Anderson LAWRENCE ANDERSON Digitally signed by LAWRENCE ANDERSON Date: 2021.07.29 08:41:53 -04'00' Office: US Department of Commerce Phone: 202-482-4444 Email: Landerson@doc.gov Signature: Date signed:
Bureau Chief Privacy Officer Name: Maria D. Dumas Office: Office of Privacy and Open Goverment Phone: 202-482-5153 Email: mDumas@doc.gov Signature: MARIA STANTON-DUMAS Digitally signed by MARIA STANTON-DUMAS Date: 2021.09.21 17:26:38 -04'00' Date signed:	