Template Version Number: 01-2020

U.S. Department of Commerce
Office of the Secretary

Privacy Impact Assessment

for the

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

Reviewed by: Maria D. Dumas, Bureau Chief Privacy Officer

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Jennifer Goode 11/18/2021

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment

Office of the Secretary / Workers Compensation Claims Medical Case Management System (WC-CMCMS)

Unique Project Identifier: OS-062

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

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 way the system operates to achieve the purpose(s) identified in Section 4
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.

(e) How information in the system is retrieved by the user
WC-CMCMS users must possess a valid need-to-know before they are granted access to their component information in WC-CMCMS. All authorized users receive remote access to

the system via an encrypted (HTTPS) session and multifactor authentication. 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 Federal Employees' Compensation Act (FECA) in accordance with the Privacy Act. A designated contract employee could be for example a nurse or a workers' compensation claims specialist. These individuals access the system to retrieve data via encrypted Citrix sessions, and multi-factor authentication (MFA) via Duo Security. System, network, and data administrators performing maintenance on the system use a virtual private network (VPN) and MFA via Entrust.

(f) 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 the 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.

(g) Any information sharing conducted by the system

WC-CMCMS shares daily eligibility files with Optum, which Optum uses to provide continuing pharmacy benefits as part of WCSP Pharmacy Benefits Manager (PBM) program provided by Optum. There is an Interconnection Security Agreement (ISA) in place that covers the data exchange methodology and controls implemented to protect PII/BII. Information is shared with DOL also.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

The WC-CMCMS receives its authority to collect, maintain, use, and disseminate user information from the Office of the Secretary of Commerce. Department Administrative Order (DAO) 202-810, 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).

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

The WC-CMCMS is categorized a Moderate system according to Federal Information Processing Standards (FIPS) 199.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.

_____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

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.

____ 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).

__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).

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*	X	f. Driver's License		j. Financial Account	
b. Taxpayer ID		g. Passport		k. Financial Transaction	
c. Employer ID		h. Alien Registration		l. Vehicle Identifier	
d. Employee ID	X	i. Credit Card		m. Medical Record	X
e. File/Case ID	X				
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, 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 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.					

General Personal Data (GPD)					
a. Name	X	h. Date of Birth	X	o. Financial Information	
b. Maiden Name		i. Place of Birth	X	p. Medical Information	X
c. Alias		j. Home Address	X	q. Military Service	
d. Gender	X	k. Telephone Number	X	r. Criminal Record	
e. Age	X	l. Email Address	X	s. Physical Characteristics	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	
b. Job Title	X	f. Salary	X	j. Proprietary or Business Information	
c. Work Address	X	g. Work History		k. Procurement/contracting records	
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance			

		Information			
l. Other work-related data (specify): Place, date, cause of injury, supervisors' names and doctors' name.					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording		i. Height	X	n. Retina/Iris Scans	
e. Photographs		j. Weight	X	o. Dental Profile	
p. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	X
b. IP Address	X	f. Queries Run	X	f. Contents of Files	X
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax	X	Online	X
Telephone	X	Email	X		
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	X
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify): Treating healthcare providers. NB: Treating physicians do not have access to ECOMP information					

2.3 Describe how the accuracy of the information in the system is ensured.

Information is collected from many sources including verbal or written communications. All data pertaining to claimant is verified with the claimant at time of collection. WC-CMCMS system does not automatically enroll claimants in the WC program but ensures claimants "opt-in" at the time of filing a claim for work-related injury or illness. This allows for verification of information stored in the system. As part of protecting data from unauthorized access, modification, or use, WC-CMCMS is housed in a federally accredited FedRAMP database which meets assurances for confidentiality, integrity, and availability.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
X	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

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

X	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	X
For administrative matters		To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The WC-CMCMS system collects, maintains and/or disseminates Personally Identifiable Information (PII) in furtherance of and as part of the WCSP to assist the DOC with medical review and oversight of all WC claims to ensure injured workers (claimants) receive timely and appropriate medical care. All claimant information including PII is entered into the DOL's ECOMP system, from where they are retrieved and manually entered into WC-CMCMS by WCSP claim specialists. This information is then supplemented by additional information (which may include PII) gathered by the Medical Case Manager. Access to the PII/BII within WC-CMCMS is restricted to authorized personnel only. All PII collected, maintained, and disseminated by WC-CMCMS system pertain and relate to only DOC employees injured at work or otherwise being treated for work-related injury.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

DOC Bureau Workers' Compensation Coordinators (WCCs) have access to WC-CMCMS and may only see data from their own bureau. There is also the potential for insider threat. All users accessing WC-CMCMS system must be authorized and possess a valid need to know before receiving access. Users are provided organizationally approved training on the system prior to receiving access, and are subject to a confidentiality or non-disclosure agreement. In addition, access to PII/BII is restricted to authorized personnel only.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau			X
DOC bureaus	X		X
Federal agencies	X		
State, local, tribal gov't agencies	none	none	none
Public	None	None	none
Private sector	X	X	none
Foreign governments	none	none	none
Foreign entities	none	none	none
Other (specify):	none	none	none

	The PII/BII in the system will not be shared.

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
X	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII. *
	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

* There should be no re-dissemination of PII/BII once it reaches DOL and Optum.

6.3 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: WC specialists uses a Pharmacy Benefits Manager (PBM) provided by Optum. Optum provides prescription drug coverage for new and ongoing workers' compensation claims. Before a claims is filed, Optum provides First Fill Card, which allows claimants to fill initial prescriptions at no cost. After a claim is filed, WC-CMCMS shares a daily eligibility file with Optum, which Optum uses to provide continuing pharmacy benefits, including a pharmacy card and mail order prescriptions. There is an Interconnection Security Agreement (ISA) that covers the data exchange methodology and controls implemented to protect PII/BII. WCSP uses SFAX (an electronic FAX service) to manage faxing. SFAX allows faxes to be securely transmitted directly to WC-CMCMS, where it is then attached to the claim file. There is an ISA that covers the data exchange methodology and controls implemented to protect PII/BII.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://www.dol.gov/sites/dolgov/files/owcp/regs/compliance/ca-1.pdf; see also https://www.commerce.gov/about/policies/privacy	
	Yes, notice is provided by other means.	Specify how:
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Injured workers are not automatically enrolled in the WC Program; they must "opt-in" at the time they claim a work-related injury or illness by completing a DOL/OWCP claim form for file a claim electronically in the DOL/OWCP provided ECOMP system. Failure to disclose the requested information may result in a delay or denial of a claim. It is the legal right of the injured worker to file a WC claim; individuals provide consent to use the information when they sign their claim form, thus initiating a workers compensation claim. This is clearly stated on the WC claim form. As contractors to DOC, the WC-MCMS Program is permitted to review claim related clinical information under the provisions of the FECA in accordance with the Privacy Act. Employees are not required to file a claim, and they may also choose to communicate directly with DOL. Employees may decline ongoing communications with the WCSP, without any detriment to their claim.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: Individuals provide consent to use the information (including PII) when they sign their claim form. This is clearly stated on the WC claim form. The reasons are stated in 7.2.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: To update PII, an individual would have to contact the WC Claims Service contract and talk directly to a claims specialist who would have authorization to use the system.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

X	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Authorized users are closely tracked in a Medical Case Management Service database.
X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 03/25/2021 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
X	Contracts with customers establish DOC ownership rights over data including PII/BII.
X	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

All electronic data exchange information between third-party WC-CMCMS user (for e.g. Optum Workers' Comp and WC-CMCMS) is encrypted in transit via AES 256-bit encryption and with static private keys. WC-CMCMS has a controlled, one-way trust relationships with its interconnected systems. At no time can either external information system initiates data transfer with WC-MCMS. WC-CMCMS users are instructed to not share identification or authentication materials of any kind, nor allow any other person to operate any DOC system by employing the user's identity.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

_X___ Yes, the PII/BII is searchable by a personal identifier.

____ No, the PII/BII is not searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: • DOL/GOVT -1- Office of Worker's Compensation Programs, Federal Employees' Compensation Act File, January 11, 2012, 77 FR 1738 • OPM/GOVT-10 - Employee Medical File System Records, June 21, 2010, 75 FR 35099
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: Personnel Injury Files General Records Schedule published by NARA, N1-GRS-86-4 item 32
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	
Degaussing	X	Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
X	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact level. *(Check all that apply.)*

X	Identifiability	Provide explanation: The system stores SSN information.
X	Quantity of PII	Provide explanation: The system collects data for users that have been injured, based on the number of cases filed for injuries and illness, and number of long term cases. There could be a couple of hundred new cases, up to 4oo or so long term cases.
X	Data Field Sensitivity	Provide explanation: This information may include name; 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.
X	Context of Use	Provide explanation: MCA advisors periodically provides statistical injury analyst reports.
X	Obligation to Protect Confidentiality	Provide explanation: MCA adheres to the Privacy Act of 1974, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies.
X	Access to and Location of PII	Provide explanation: All PII is located in the WebOPUS. DOC Bureau Workers' Compensation Coordinators (WCCs) have access to WC-CMCMS and may only see data from their own bureau. There is also the potential for insider threat. All users accessing WC-CMCMS system must be authorized and possess a valid need to know before receiving access. Users are provided organizationally approved training on thesystem prior to receiving access, and are subject to a confidentiality or non-disclosure agreement. In addition, access to PII/BII is restricted to authorized personnel only. MCA designated employees have access to the system.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

DOC Bureau Workers' Compensation Coordinators (WCCs) have access to WC-CMCMS and may only see data from their own bureau. There is also the potential for insider threat. All users accessing WC-CMCMS system must be authorized and possess a valid need to know before receiving access. Users are provided organizationally approved training on the system prior to receiving access, and are subject to a confidentiality or non-disclosure agreement. In addition, access to PII/BII is restricted to authorized personnel only.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

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

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: STEWART MERRITTS Digitally signed by STEWART MERRITTS Date: 2021.07.28 10:49:21 -04'00'

Date signed: _____

Information Technology Security Officer

Name: Jerome Nash
Office: US Department of Commerce
Phone: 202-482-5929
Email: Jnash@doc.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: JEROME NASH Digitally signed by JEROME NASH Date: 2021.07.28 11:46:03 -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

I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA.

Signature: TAHIRA MURPHY Digitally signed by TAHIRA MURPHY Date: 2021.09.13 12:16:16 -04'00'

Date signed: _____

Authorizing Official
Name: Lawrence W. Anderson
Office: US Department of Commerce
Phone: 202-482-4444
Email: Landerson@doc.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: LAWRENCE ANDERSON Digitally signed by LAWRENCE ANDERSON Date: 2021.07.29 08:38:59 -04'00'

Date signed: _____

Bureau Chief Privacy Officer
Name: Maria Dumas
Office: Office of Privacy and Open Government
Phone: 202-482-5153
Email: mDumas@doc.gov

I certify that the PII/BII processed in this IT system is necessary and this PIA ensures compliance with DOC policy to protect privacy.

Signature: MARIA STANTON-DUMAS Digitally signed by MARIA STANTON-DUMAS Date: 2021.09.21 17:54:33 -04'00'

Date signed: _____

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.