U.S. DEPARTMENT OF LABOR

Office of the Chief Information Officer

PRIVACY IMPACT ASSESSMENT
COST DETERMINATION INFORMATION MANAGEMENT SYSTEM (CDIMS)

VERSION 1.8

4/20/2022

DOCUMENT CHANGE HISTORY

Date	Filename / Version #	Author	Revision Description
11/19/08	Privacy Impact Assessment Template 1.5	Adrienne Ramirez	Annual Update
05/01/10	Privacy Impact Assessment	Adrienne Ramirez, Michael O'Rourke	Annual Update
01/07/11	Privacy Impact Assessment	Adrienne Ramirez	Appendix A
3/12/12	Privacy Impact Assessment	Adrienne Ramirez	To include 3rd Party Website Updates
2/25/13	Privacy Impact Assessment	Adrienne Ramirez	Annual Review
12/16/15	Privacy Impact Assessment	Adrienne Ramirez	Review and Update
12/16/16	Privacy Impact Assessment	Adrienne Ramirez	Review and Update
12/18/17	Privacy Impact Assessment	Adrienne Ramirez	Review and Update
12/17/18	Privacy Impact Assessment	Adrienne Ramirez	Annual Review and Update
11/27/20	Privacy Impact Assessment	Adrienne Ramirez	Annual Review and Updates

DOCUMENT REVIEW HISTORY

Date	Version #	Reviewers
11/19/08	Privacy Impact Assessment Template 1.5	Tonya Manning
06/10/10	Privacy Impact Assessment Template 1.6	Tonya Manning
01/07/11	Privacy Impact Assessment Template 1.6	Tonya Manning
03/12/12	Privacy Impact Assessment Template 1.7	Tonya Manning
03/01/13	Privacy Impact Assessment Template 1.7	Tonya Manning
12/16/15	Privacy Impact Assessment Template 1.8	Miranda Key

12/16/16	**Privacy Impact Assessment Template 1.8**	**Adrienne Ramirez**
12/20/17	**Privacy Impact Assessment Template 1.8**	**Adrienne Ramirez**
12/18/18	**Privacy Impact Assessment Template 1.8**	**Adrienne Ramirez**
11/27/20	**Privacy Impact Assessment 1.8**	**Adrienne Ramirez**
2/16/22	**Privacy Impact Assessment**	**Victor Lopez**
2/23/22	**Privacy Impact Assessment**	**Jennifer Fox**
2/25/22	**Privacy Impact Assessment**	**Victor Lopez**
4/20/22	**Privacy Impact Assessment**	**DSAM**

TABLE OF CONTENTS

1.1 OVERVIEW

The Department of Labor (DOL) relies on the Cost and Price Determination Division (CPDD) Cost Determination Information Management System (CDIMS), to accomplish its mission of providing cost-effective and reliable services to the DOL, and the public at large. CDIMS is a Salesforce Software as a Service (SaaS) application which is owned and managed by the Office of the Assistant Secretary for Administration and Management (OASAM).

CDIMS serves to support the CPDD in negotiating and issuing indirect cost rates (ICR) and cost allocation plans (CAPs) on behalf of the Federal Government, for organizations receiving the preponderance of direct Federal funds from the U.S. Department of Labor (DOL). The CDIMS team works with grantees, the point of contact (POC) for those companies and organizations, to receive the direct Federal funds. The negotiated ICR rates and CAPs are utilized to properly support indirect cost billings and close-out efforts on cost reimbursable grants and contracts. CDIMS issues letters and Negotiated Indirect Cost Rate Agreements (NICRAs) to non-Federal entities seeking indirect cost proposal approvals. A privacy impact assessment (PIA) is being completed as the system collects and stores non-sensitive PII on members of the public.

1.2 CHARACTERIZATION OF THE INFORMATION

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

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

- From whom is information to be collected?

  PII is collected on members of the public who work at the companies/businesses submitting cost reimbursable grants and contracts as well as Federal employees and contractors that use the system.

- Why is the Information being collected?

  PII is collected because CDIMS requires a point of contact (POC) to communicate with the grantee/contractor on any proposals submitted to DOL. These proposals are reviewed and Negotiated Indirect Cost Rate Agreements (NICRAs) are negotiated for all non-Federal entities.

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

  The type of information collected from Federal employees and contracting staff includes: First and Last Names, Business Email Address, Business Phone Numbers
  The type of information collected from the Public include: First and Last Names, Business email address, business phone number, business address

- How is the PII collected?

  The PII is being collected through submitted proposal packages via email. The company/business will submit a POC and their information to respond to inquiries or requests from the CDIMS team.

- How will the information collected from individuals or derived from the system be checked for accuracy?

  The information collected is submitted by the company/business. The information is not reviewed or checked for accuracy unless the company/business inform the CIDMS team that there is an update in the POC via email.

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

  The authority permitting collection of PII is, 2 Code of Federal Regulations (CFR) 200, Appendix IV and VII; and Federal Acquisition Regulation (FAR) 42.7. These authorities require the submission of indirect cost proposals on an annual basis to Federal cognizant agencies, such as CPDD. The proposals are submitted by email and typically include a cover letter providing POC information in case we have any questions. The NICRAs are emailed back to the non-Federal entity's POC after the review and approval process.

- Privacy Impact Analysis

  CDIMS has very few users who are able to access and review the PII within the system. Authentication and access controls within CDIMS will prevent unauthorized individuals from gaining access to the PII within the system. User accounts are reviewed on a monthly and semi-annually basis to ensure no users have access to the PII within the system that aren't supposed to. Additionally, all DOL personnel will be required to sign a Rules of Behavior agreement to ensure they understand and acknowledge their responsibilities regarding the handling and protection of PII.

1.3 DESCRIBE THE USES OF THE PII

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

- Describe all the uses of the PII

  The PII is used by the CDIMS user to communicate and negotiate indirect costs with the non-Federal entity.

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

  No tool is analyzed or produced within CDIMS. The PII collected is strictly to be used for communication and negotiation of indirect cost proposals.

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

  CDIMS does not derive new data or PII from what is collected through the submitted proposals.

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

  CIDMS uses publicly available data; The majority of the information received from the POC is business related (email, address, and phone number) and limited personal PII is captured within CDIMS.

- Will the use of PII create or modify a "system of records notification" under the Privacy Act?

  No, the PII does not create or modify a system of records notification (SORN) as described in the Privacy Act.

- Privacy Impact Analysis

  CDIMS is a FedRAMP NIST Moderate system and has implemented all Privacy related controls within the NIST baseline. These controls include documentation, legal authority, use of PII, and retention of PII controls that allow the CDIMS team to properly secure and reduce the risk of PII within the system. Additionally, all DOL personnel will be required to sign a Rules of Behavior agreement to ensure they understand and acknowledge their responsibilities regarding the handling and protection of PII.

1.4 RETENTION

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

- What is the retention period for the data in the system?

  We follow the "highest" requirement to ensure no issues with record retention as described below:

  1. DOL records management team (GENERAL RECORDS SCHEDULE 1.2 – Transmittal No.23, September 2014). In it, states that we keep files for at least 10 years from closure.

- Is a retention period established to minimize privacy risk?

  CDIMS follows the "highest" retention period as defined above to ensure proper procedures to applicable FAR, CFR, and DOL records management policies are being addressed.

- Has the retention schedule been approved National Archives and Records Administration (NARA)?

  The NARA retention schedule number is DAA-GRS-2013-0008-0001.

- Per M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*; what efforts are being made to eliminate or reduce PII that is collected, stored or maintained by the system if it is no longer required?

  CDIMS stores all PII with its respective proposal. Proposals are required to be retained for 10 years per the NARA schedule. After 10 years, the CDIMS team will review the proposal to determine if it is needed or can be eliminated.

- Have you implemented the DOL PII Data Extract Guide for the purpose of eliminating or reducing PII?

  PII is extracted when the system team issues cover letters and NICRAs. PII non-sensitive POC information is included to be able to properly deliver email correspondence to the non-Federal entity. Audit logs are tracked a reviewed monthly for CDIMS and the system team reviews all outputs to ensure only necessary PII is included.

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

  After the 10-year period from closure, if it is deemed there is no longer a business need for the information, the PII will be eliminated

- If you are unable to eliminate PII from this system, what efforts are you undertaking to mask, de-identify or anonymize PII.

  CDIMS does not request any additional PII from the company/business. The only PII that is within the system is the PII POC information that is submitted with each proposal. All PII within the system is associated with a proposal and is not used unless necessary for communication purposes.

- Privacy Impact Analysis

  CDIMS only stores PII that is necessary for their business and mission purpose. CDIMS users are required to have a notice within their emails that states no PII should be submitted to them that is not necessary to fulfill their question or request. Although PII is kept within the system for at least 10 years, closed proposals are only viewed to help with future proposals with the same grantee or company. These closed records are not viewed or distributed for any reason other than to help with future business and mission purposes.

1.5 INTERNAL SHARING AND DISCLOSURE

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

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

  No information is shared outside of the CDIMS system which is used by the Cost & Price Determination Division (CPDD) within the Office of the Senior Procurement Executive (OSPE). All users of CDIMS are internal DOL employees from the OSPE agency or contractors used to help develop the system.

- How is the PII transmitted or disclosed?

  CDIMS PII is not transmitted or disclosed to any internal agencies or systems. PII is only viewed and used to communicate with the grantee that submitted a proposal.

- Does the agency review when the sharing of personal information is no longer required to stop the transfer of sensitive information?

  No information is shared from the CDIMS system to internal agencies or systems. It is determined that after a proposal is closed, the PII is no longer needed to be transferred.

- Privacy Impact Analysis

  CDIMS does not share any information or PII with internal agencies or systems. PII is only used to communicate with the grantee for a given proposal. Once the proposal is closed, the PII is no longer viewed, used, or shared with any internal or external organizations.

1.6 EXTERNAL SHARING AND DISCLOSURE

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

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

  CDIMS issues letters and NICRAs to non-Federal entities seeking indirect cost proposal approvals. These documents need to have PII non-sensitive POC information to be able to be mailed or emailed to the non-Federal entity. The POC information includes name and business addresses.

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

  The sharing of PII is compatible with the original collection. A SORN is not required by CDIMS as records are not retrieved using a personal identifier.

  The regulations at 2 CFR 200, Appendix IV, C.2.g., and FAR 42.706 require the issuance of NICRAs after completing indirect cost negotiations with non-Federal entities. These agreements, signed by two parties (non-Federal entities and this office on behalf of the Federal government), have limited POC information for first name, last name, and title.

  The above regulations also require that these documents be made available to all concerned Federal agencies.

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

  The documents are emailed to the non-Federal entity or concerned Federal agency. PII can only be emailed via a DOL email address.

- How is the information transmitted or disclosed?

  The documents are emailed to the non-Federal entity. PII can only be emailed via a DOL email address.

- Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement

reflect the scope of the information currently shared? If the answer is yes, be prepared to provide a copy of the agreement in the event of an audit as supporting evidence.

A MOU is not required by CDIMS as there are no external connections to other systems. The regulations at 2 CFR 200, Appendix IV, C.2.g., and FAR 42.706 require the issuance of NICRAs after completing indirect cost negotiations with non-Federal entities. These agreements, signed by two parties (non-Federal entities and this office on behalf of the Federal government), have limited POC information for first name, last name, and title.

The above regulations also require that these documents be made available to all concerned Federal agencies.

- How is the shared information secured by the recipient?

  The information is shared by the recipient through email to the non-federal entities. PII can only be emailed via a DOL email address.

- What type of training is required for users from agencies outside DOL prior to receiving access to the information?

  Training is not provided as the non-federal entities are given documents and do not have access into the system to update or modify any data.

- Privacy Impact Analysis

  CDIMS does not allow access within the system by any external users to help minimize privacy risk. All information and data can only be accessed by internal DOL users. CDIMS only uses PII POC information to be able to communicate and negotiate with non-Federal entities.

1.7 NOTICE

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

- Was notice provided to the individual prior to collection of PII? If yes, please provide a copy of the notice as an appendix or be prepared to provide a copy of the notice during an audit request. A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice. If notice was not provided, please explain.

  A notice is not provided to the individual prior to collection of PII. The Company/businesses reach out to the CDIMS team to submit a proposal, which contains the POC's information and PII. After a proposal is received, if the CDIMS user requires further information or clarification, they will reach out to the POC given by the company/business. During this reach out, each CDIMS user contains a PII notice within the email that states:

  "*The information transmitted is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged material. Any review, retransmission, dissemination, or other use of, or taking of any action in reliance upon, this information by persons or entities other than the intended recipient is prohibited. Notify sender if this email was received in error. For customers: Ensure that* ***no*** *personal identifiable information (PII; Ex. social security numbers) are provided when submitting documentation.*"

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

  The company/businesses submit a POC's information to the CDIMS team with a proposal with the sole intent to reach out if there are any questions or updates required.

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

  The company/businesses= submit a POC's information to the CDIMS team with a proposal with the sole intent to reach out if there are any questions or updates required.

- Privacy Impact Analysis

  CDIMS only requires the least amount of PII (Name, business email, business address, business phone number) to be collected by the individuals. This information is only used in case of questions or updates to the proposal. Additionally, there is a notice in all CDIMS users' emails to make sure no additional PII is collected by accident to help minimize the amount of PII collection within the system.

1.8 INDIVIDUAL ACCESS, REDRESS, AND CORRECTION

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

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

  Only CDIMS authorized users are allowed to access the PII within the system. Individuals are not allowed to access their personal PII.

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

  If the POC provided by the business/company needs to be changed, it is assumed the current POC will notify the CDIMS team prior to their departure. The CDIMS team will then update the information within the system.

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

  Individuals are allowed to correct their information by reaching out to a CDIMS authorized users.

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

  Individuals are allowed to correct their information by reaching out to a CDIMS authorized user. It is assumed the current POC associated with the proposal will notify the CDIMS team prior to their departure that their will be a new POC for the proposal.

- Privacy Impact Analysis

  PII within CDIMS can only be accessed by CDIMS authorized users which are all internal DOL employees or contractors. The information can be updated at any time if a proposal requires a new POC to answer any questions or requests. To mitigate the risk of inaccurate PII within the system, CDIMS users allow the POC to correct them on any misinformation provided and by proactively letting them know they are no longer the correct POC for the given proposal.

1.9 TECHNICAL ACCESS AND SECURITY

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

- Which user group(s) will have access to the system? (For example, program managers, IT specialists, and analysts will have general access to the system and registered users from the public will have limited access.)

  CDIMS authorized users are allowed access into the system. The different groups within CDIMS are System Administrators and General Users.

- Will contractors to DOL have access to the system? If so, please include a copy of the contract describing their role to the OCIO Security with this PIA or be prepared to provide copies during an audit request

  DOL contractors will have access into the system. They are not authorized to add or modify any PII or data within the system. They provide Salesforce IT support to update any configuration changes that are needed by the System Administrators within the system. A copy of the contract agreement will be provided in the case of an audit request.

- Does the system use "roles" to assign privileges to users of the system? If yes, describe the roles.

  CDIMS has defined roles and responsibilities for each user within their Account Management Standard Operating Procedures (SOP). The two types of roles are general users and system administrators. General Users have access to read, update, and upload information into the system. System Administrators have access to all general user functionality as well as account, audit, and configuration management.

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

  CIDMS has documented their account management processes and roles within the Account Management SOP. A user that wants to access the system must submit a System Access Request (SAR) form.

- How are the actual assignments of roles and Rules of Behavior, verified according to established security and auditing procedures? How often training is provided. Provide date of last training.

  A user must submit a SAR form which details the account type they are requesting and a Rules of Behavior that must be reviewed. The review process and who can sign off on the SAR form is documented in the CDIMS Account Management SOP. These documents are kept by the system team for audit purposes. Training is provided to all

users when they first receive an account within CDIMS. Additionally, all users complete an annual IT security and awareness training via Learning Link.

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

  Privacy training is provided on an annual basis via Learning Link to all DOL employees. Additionally, training is provided by the System Administrator when a user first receives an account.

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

  CDIMS is only used by internal authorized users, and they must be on the DOL VPN to access the system. The system provides audit logs which are reviewed monthly by the system team.

- Is the data secured in accordance with FISMA requirements? If yes, when was Security Assessment and Authorization last completed?

  CDIMS is a Salesforce Software as a Service (SaaS) and is FISMA certified.

- Privacy Impact Analysis

  CDIMS is only used by internal DOL authorized users. The system can only be accessed while on the DOL network. Since CDIMS is a Salesforce based system, information is encrypted at rest and in transit per Salesforce FedRAMP Package.

1.10 TECHNOLOGY

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

- Was the system built from the ground up or purchased and installed?

  CDIMS was purchased and installed.

- Describe how data integrity, privacy and security were analyzed as part of the decisions made for your system.

  CDIMS is a Salesforce FedRAMP cloud service provider. While during implementation, CDIMS implemented SSO and IP restrictions to limit the access into the system. CDIMS limits the number of user accounts within the system to allow the least number of users necessary into the system. Privacy and Security were analyzed as part of the implementation of CDIMS as described in the contract agreement to develop the system.

- What design choices were made to enhance privacy?

  CDIMS implemented SSO and IP restrictions to limit the access into the system to only those individuals that are required to review and view the PII within the system. The CDIMS team does not collect any more PII than is necessary to complete its business and mission purposes.

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

  CDIMS is operational.

- For systems in development, does the project employ technology that may raise privacy concerns? If so, please discuss their implementation?

  CDIMS is operational.

1.11 DETERMINATION

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

OSPE has completed the PIA for CDIMS which is currently in operation. OSPE has determined that the safeguards and controls for this Moderate system adequately protect the information.

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

1.12 PIA SIGNATURE PAGE

Responsible Officials

Timothy Erskine
System Owner

TIMOTHY ERSKINE Digitally signed by TIMOTHY ERSKINE Date: 2022.04.22 15:58:03 -04'00'

_____ _____

Signature of System Owner *Date*

APPENDIX A: DEFINITIONS FOR PII AND PII ELEMENTS THIS SYSTEM COLLECTS

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

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

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

- ☒ Prefix or title, such as Mr., Mrs., Ms., Jr. Sr. ☐
- ☒ First name ☐ Middle initial and/or ☒ Last name
- ☐ Name suffix such as Jr. Sr., etc.
- ☐ Date of birth
- ☐ Place of birth
- ☐ Mother's maiden name
- ☐ SSN
- ☐ SSN [truncated]
- ☐ SSN [elongated]
- ☐ Language spoken
- ☐ Military, immigration, or other government-issued identifier
- ☐ Photographic identifiers (i.e., photograph image, x-rays, video)
- ☐ Biometric identifier (i.e., fingerprint, voiceprint, iris)
- ☐ Other physical identifying information (e.g., tattoo, birthmark)
- ☐ Vehicle identifier (e.g., license place, VIN)
- ☐ Driver's license number
- ☐ Residential address
- ☒ Personal phone numbers (e.g., phone, fax, cell)

- ☐ Mailing address (e.g., P.O. Box)
- ☐ Personal e-mail address
- ☒ Business address
- ☒ Business phone number (e.g., phone, fax, cell)
- ☒ Business e-mail address
- ☐ Medical information including physician's notes
- ☐ Medical record number
- ☐ Device identifiers (e.g., pacemaker, hearing aid)
- ☒ Employer Identification Number (EIN)/Taxpayer Identification Number (TIN)
- ☐ Financial account information and/or number (e.g., checking account number, PIN, retirement, investment account)
- ☐ Certificates (e.g., birth, death, marriage)
- ☐ Legal documents or notes (e.g., divorce decree, criminal records)
- ☐ Educational records
- ☐ Network logon credentials (e.g., username and password, public key certificate)
- ☒ Digital signing or encryption certificate
- ☐ Other: _____
- ☐ None

- Is any part of the PII collection voluntary?

  All PII collected is within CDIMS is submitted to by the company/business who submitted a proposal to the CDIMS team.

- If any part of the PII collection is voluntary, what efforts are being made to redact, mask, anonymize or eliminate PII from this system?

  CDIMS does not request any additional PII from the company/business. The only PII that is within the system is the PII POC information that is submitted with each proposal. All PII within the system is associated with a proposal and is not used unless necessary for communication purposes. Once a proposal is completed, the PII is no longer used.