U.S. DEPARTMENT OF LABOR

Office of Federal Contract Compliance Programs (OFCCP)

COMPLIANCE MANAGEMENT SYSTEM (CMS-OFCCP)

PRIVACY IMPACT ASSESSMENT

VERSION 1.4

DOCUMENT CHANGE HISTORY

Date	Filename / Version #	Author	Revision Description
3/12/19	CMS-OFCCP PIA / Version 1.0	R. Fuller	Initial
5/21/19	CMS-OFCCP PIA / Version 1.1	CollabraLink Technologies Inc.	Response to OCIO comments
11/16/22	CMS-OFCCP PIA / Version 1.2	S. Montiel, S. Lee	DSAM Comments for Renewal Updates
5/11/2023	CMS-OFCCP PIA / Version 1.3	S.Montiel	Additional updates per SORN
6/8/2023	CMS-OFCCP PIA / Version 1.4	V.Lingam	Verification of CMS-OFCCP information

DOCUMENT REVIEW HISTORY

Date	Version #	Reviewers
11/16/22	CMS-OFCCP PIA / Version 1.2	S. Montiel, S. Lee
5/11/2023	CMS-OFCCP PIA / Version 1.3	S.Montiel
6/8/2023	C4S-OFCCP PIA / Version 1.4	V.Lingam

TABLE OF CONTENTS

PRIVACY IMPACT ASSESSMENT QUESTIONNAIRE

1.1 OVERVIEW

The Office of Federal Contract Compliance Programs, Compliance Management System (CMS-OFCCP) is a web-based application built on Appian, hosted on the Amazon Web Services (AWS) GovCloud environment that supports a set of automated tools used to collect data, track, plan, and report on the compliance evaluations and investigations OFCCP conducts to ensure that the laws the program administers are enforced.

AWS GovCloud (US) is an AWS region designed to allow United States (US) government agencies at the federal, state and local level, along with contractors, educational institutions and other US customers to run sensitive workloads in the cloud by addressing their specific regulatory and compliance requirements. Beyond the assurance programs applicable to all AWS regions, the AWS GovCloud region allows customers to adhere to Federal Risk and Authorization Management Program (FedRAMP) requirements.

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.

CMS-OFCCP collects information on Federal contractors and Federal contract businesses. CMS-OFCCP supports tracking investigation cases. This may include files related to the case. All information collected is about federal contractors and their employees.

- From whom is information to be collected?

  Individuals filing complaints with OFCCP of employment discrimination by Federal Contractors and Compliance Officers. Individuals, Companies, classes of individuals or representatives authorized to act on behalf of individuals or classes of individuals who have filed complaints of discrimination.

- Why is the information being collected?

  Information is being collected to support the tracking and reporting on investigation cases.

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

  The information collected from the companies are anonymous in nature. Eg: 30% female,

50 veterans etc. There is no PII details about names or age/sex/veteran/disability status of the employee that is exchanged. The information collected from an individual when they lodge a discrimination complaint is their contact information, Age/Sex/Race/Disability status/Veteran Status and medical records.

The PII that is collected as a part of compliance evaluation process are the following:

- Applicant and Employee Hiring Data
- Contact Information (First Name, Last Name)
- Demographic Information (Sex, Race, Veteran, Disability) *This is future state. Currently we are not collecting this data.*
- Medical records, investigative reports and materials, complaints, contract coverage information, employment applications, time and attendance records. *This is future state. Currently we are not collecting this data.*
- Listing of complaints filed by individuals alleging employment. *This is future state as well.*

- How is the PII collected?

DOL CMS-OFCCP does not collect PII directly from individuals. Information contained in this system is obtained from OFCCP personnel working in district and regional offices. Complaint Case File is obtained from individual and class action complainants, employers, co-workers, witnesses, State rehabilitation agencies, physicians, and other health care providers. PII for the compliance evaluation is collected from the POC (Federal Contractor Company) identified as a part of the compliance evaluation process conducted on the federal contractor's facility.

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

The data collected is provided by the Federal Contractor Company. We assume that the information coming from the company is correct.

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

The legal authority that defines and provides for the maintenance of PII in CMS-OFCCP is Executive Order 11246, as amended; the Vietnam Era Veterans' Readjustment Assistance Act of 1974, as amended, 38 U.S.C. 4212; section 503 of the Rehabilitation Act of 1973, as amended, 29 U.S.C. 793.

- Privacy Impact Analysis

The risks identified are directly related to the collection and use of the PII by designated OFCCP personnel nationwide. The only users that have direct access to this information

are OFCCP compliance officers, designated OFCCP authorized users, and CMS-OFCCP operations teams. These employees are responsible for conducting the evaluations and investigations in support of the mission of the OFCCP. Possible risks include the following:

- Inappropriate use of the PII collected
- Failure to secure any hardcopy documents on which PII appears
- Malicious theft of data by a motivated outside attacker.

The mitigations actions that are currently employed to reduce the potential of exposure of the identified PII are the following:

- Establish and provide secure access to the CMS-OFCCP
- Establish and provide secure access to all OFCCP office locations
- Establish and provide secure storage of hardcopy documentation in OFCCP offices
- Conduct annual training to all OFCCP employees and contractors on OFCCP employees' responsibilities for protection all information received (electronic and non-electronic) from federal contractors
- Provide access to and training for the proper disposal (shredding and/or burning) of all hardcopy documents prior to disposal and/or for the destruction of all electronic portable media (CDs, USB Drives, Memory Cards, etc.) received or used during the investigation and evaluation processes conducted by the OFCCP. This includes the acquisition and use of shredding devices at all OFCCP office locations.
- Minimize all data collection to the minimum necessary to conduct investigations.
- Avoid shipping documents whenever feasible. Enforce rigorous standards when shipping or mailing documents.

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 intended to be used by compliance officers conducting either compliance evaluations or complaint investigations. While this PII is stored in CMS-OFCCP, it is not included as data on any of the reports accessible to end users of this information system. With the exception of the PII collected during the complaint investigation process, this information does not appear on any of the pre-formatted reports that are available within CMS-OFCCP.

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

  Microsoft products (excel) and Statistical tools (SAS, R) are used to produce aggregate statistical results

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

  No.

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

  Publicly Available Data is used as follows:
  - Melissa is used for address validation
  - Census data for NAICS codes validation
  - Metropolitan Statistical Area (MSA) data for Geographic Reference Information
  - USASpending.gov for federal contractor information and contract details

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

  Yes. Information contained in CMS-OFCCP is covered by a System of Records Notice (SORN) as defined by the Privacy Act of 1974.

  CMS-OFCCP leverages the following SORN:
  - DOL/OFCCP-I, Office of Federal Contract Compliance Programs, Executive Management Information System (OFCCP/EIS)
  - DOL/OFCCP-2, Office of Federal Contract Compliance Programs/Complaint Case Files.

- Privacy Impact Analysis

  The risks identified are directly related to the collection and use of the PII by designated OFCCP personnel nationwide. The only users that have direct access to this information are OFCCP compliance officers, designated OFCCP authorized users, and CMS-OFCCP operations teams. These employees are responsible for conducting the evaluations and investigations in support of the mission of the OFCCP. Possible risks include the following:

  1. Inappropriate use of the PII collected
  2. Malicious theft of data by a motivated outside attacker.

  The mitigations actions that are currently employed to reduce the potential of exposure of the identified PII are the following:

  1. Establish and provide secure access to CMS-OFCCP through security controls
  2. Establish and provide secure access to all OFCCP office locations
  3. Conduct annual training to all OFCCP employees and contractors on OFCCP employees' responsibilities for protection all information received
  4. Minimize all data collection to the minimum necessary to conduct investigations.

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?

  Permanent. The system itself and all data within is considered a permanent record.

- Is a retention period established to minimize privacy risk?

  Yes, and to document agency operations, retention period is not enforced on CMS. All records are permanent.

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

  Yes. All data in the OFCCP Information System is a permanent record. In accordance with the agency records schedule, data is to be transferred to NARA every five calendar years in a format acceptable to NARA at the time of transfer [OFCCP Records Schedule N1-448-01-02, Item 9(a)].

- 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?

  OFCCP data requirements have been reviewed by OFCCP management and determined to be necessary for OFCCP operations. Should OFCCP operational requirements change, OFCCP management will review the data requirements with the purpose of altering the amount of PII collected, stored, or maintained by CMS-OFCCP.

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

  Data requirements are established by NARA and FOIA requirements.

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

  N/A- the information is used to directly reach points of contact and access is limited to employees responsible for working with those individuals. The information collected from the contractors are collected in an anonymous fashion. Ex: 50 of the employees are female, 30% are veterans etc.

- Privacy Impact Analysis

  The risks identified are directly related to the collection and use of the PII by designated OFCCP personnel nationwide. The only users that have direct access to this information are OFCCP compliance officers, designated OFCCP authorized users, and CMS-OFCCP operations teams. These employees are responsible for conducting the evaluations and investigations in support of the mission of the OFCCP. Possible risks include the following:

  - Inappropriate use of the PII collected
  - Failure to secure any hardcopy documents on which PII appears
  - Malicious theft of data by a motivated outside attacker.

  The mitigations actions that are currently employed to reduce the potential of exposure of the identified PII are the following:

  - Establish and provide secure access to the CMS-OFCCP
  - Establish and provide secure access to all OFCCP office locations
  - Conduct annual training to all OFCCP employees and contractors on OFCCP employees' responsibilities for protection all information received from federal contractors

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?

  The identified PII is collected through our regional, district and area office locations, as well as the national office. This information is only available internally via CMS-OFCCP reports, and the original case files.

- How is the PII transmitted or disclosed?

  The identified PII is transmitted internally between the OFCCP regional/district/area offices and the national office through CMS-OFCCP. This information is transmitted electronically and is only disclosed to those employees on a "need-to-know" basis.

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

  Not applicable; the information maintained in CMS-OFCCP to support FOIA and NARA requirements, and potential future investigations.

- Privacy Impact Analysis

  The risks identified are directly related to the collection and use of the PII by designated OFCCP personnel nationwide. The only users that have direct access to this information are OFCCP compliance officers, designated OFCCP authorized users, and CMS-OFCCP operations teams. These employees are responsible for conducting the evaluations and investigations in support of the mission of the OFCCP. Possible risks include the following:

  - Inappropriate use of the PII collected
  - Failure to secure any hardcopy documents on which PII appears
  - Malicious theft of data by a motivated outside attacker.

  The mitigations actions that are currently employed to reduce the potential of exposure of the identified PII are the following:

  - Establish and provide secure access to the CMS-OFCCP
  - Establish and provide secure access to all OFCCP office locations
  - Conduct annual training to all OFCCP employees and contractors on OFCCP employees' responsibilities for protection all information received from federal contractors

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?

  Not Applicable. The identified PII is not shared with any organizations/entities outside of the OFCCP.

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

  Not Applicable. The identified PII is not shared with any organizations/entities outside of the OFCCP.

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

  Not Applicable. The identified PII is not shared with any organizations/entities outside of the OFCCP.

- How is the information transmitted or disclosed?

  Not Applicable. The identified PII is not shared with any organizations/entities outside of the OFCCP.

- 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.

  Not Applicable. The identified PII is not shared with any organizations/entities outside of the OFCCP.

- How is the shared information secured by the recipient?

  Not Applicable. The identified PII is not shared with any organizations/entities outside of the OFCCP.

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

  Not Applicable. The identified PII is not shared with any organizations/entities outside of the OFCCP.

- Privacy Impact Analysis

  There is no risk identified with external sharing, as OFCCP does not participate in any agreements involving the transfer of PII

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. 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.

  N/A-The PII maintained in CMS-OFCCP contains complaints and investigative files compiled during complaint investigations and compliance reviews. In accordance with paragraph (k)(2) of the Privacy Act, 5 U.S.C. 552a(k)(2), these files have been exempted from subsections (c)(3),(d), (e)(1), (e)(4)(G), (H), and (I) and (f) of the Act. However, if any individual is denied any right, privilege, or benefit that he or she would otherwise be entitled to by Federal law, or for which he or she would otherwise be eligible, as a result of the maintenance of these records, such material shall be provided to the individual, except to the extent that the disclosure of such material would reveal the identity of the source would be held in confidence.

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

  N/A. See above statement

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

  N/A. See above statement.

- Privacy Impact Analysis

  N/A

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?
  Per the SORN, a request for access should be mailed to the System Manager/Owner.

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

  Upon identification/notification of the identified PII, whether associated with a compliance evaluation or a complaint investigation case record, the assigned compliance officer is responsible for correcting inaccuracies with the identified PII prior to the completion of the compliance evaluation or complaint investigation.

- How are individuals notified of the procedures for correcting their own information?
  N/A- Information is obtained from OFCCP personnel working in district and regional offices. The PII maintained in CMS-OFCCP contains complaints and investigative files compiled during complaint investigations and compliance reviews. In accordance with paragraph (k)(2) of the Privacy Act, 5 U.S.C. 552a(k)(2), these files have been exempted from subsections (c)(3),(d), (e)(1), (e)(4)(G), (H), and (I) and (f) of the Act. However, if any individual is denied any right, privilege, or benefit that he or she would otherwise be entitled to by Federal law, or for which he or she would otherwise be eligible, as a result of the maintenance of these records, such material shall be provided to the individual, except to the extent that the disclosure of such material would reveal the identity of the source would be held in confidence.

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

  Not applicable (see above)

- Privacy Impact Analysis

  N/A

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.)

  Access is limited to OFCCP employees, and the IT staff responsible for supporting the system.

- 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.

  Yes, contract support for CMS-OFCCP is provided by Appteon Inc. No contractors outside of the contract staff are provided access to the system. Contract information contains sensitive data and will only be released on "need to know" basis by System Owner upon request.

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

  Yes, CMS-OFCCP employs role-based access. Each user is given a "role" (compliance officer, district director, assistant district director, etc.), and an office location. Users can only access, modify, and view cases within the geographic region for which they arc; responsible. Managers have access to the files of their employees.

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

  There are Access Control/Account Management procedures which are currently in place that describe the technical safeguards and security measures for ensuring access to the CMS-OFCCP is managed and monitored.

- 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.

  Roles are established and managed by OFCCP managers. Managers cannot elevate a user above their own privileges. All users must complete the Rules of Behavior prior to being granted access to the system. Employees participate in mandatory Privacy Act and Records Management training annually. This is provided by Learning Link, and so no single hard date is available.

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

  Employees participate in mandatory Privacy Act and Records Management training annually. This is provided by Learning Link, and so no single hard date is available

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

  Auditing functionality is provided by OFCCP support staff and OASAM, as well as other technical safeguards to prevent the misuse of data. Technical safeguards provide user, account management, and privileged user actions to be recorded in an audit log and backed up to support after-the-fact investigations. CMS-OFCCP auditable events consist of the object being acted upon, the action being performed, the old and new value where applicable, and the individual who initiated the action. All events are time stamped.

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

  Yes. CMS-OFCCP received its initial authorization on 5/17/2019 and remains a participant in the DOL Ongoing Authorization program. Annual Security Assessments are performed as part of the Ongoing Authorization process.

- Privacy Impact Analysis

  The risks identified are directly related to the collection and use of the PII by designated OFCCP personnel nationwide. The primary OFCCP user community that has direct access to this information is the Compliance Officer Community. These employees are responsible for conducting the evaluations and investigations in support of the mission of the OFCCP. Possible risks include the following:

  - Inappropriate use of the PII collected
  - Failure to secure any hardcopy documents on which PII appears
  - Malicious theft of data by a motivated outside attacker.

  The mitigations actions that are currently employed to reduce the potential of exposure of the identified PII are the following:

  - Establish and provide secure access to the CMS-OFCCP
  - Establish and provide secure access to all OFCCP office locations
  - Conduct annual training to all OFCCP employees and contractors on OFCCP employees' responsibilities for protection all information received from federal contractors
  - Minimize all data collection to the minimum necessary to conduct investigations
  - While there are no auditing measures in place to protect the PII in the system, there are technical safeguards that restrict access to the system as previously mentioned. In

addition, users of the system have been adequately trained in the use and administration of privacy information.

1.10 TECHNOLOGY

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

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

  The system was custom-designed and built.

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

  The requirement to implement security and privacy controls were addressed in the system acquisition contract for CMS-OFCCP.

- What design choices were made to enhance privacy?

  CMS-OFCCP employs technical controls and mechanisms, such as encryption, access role, need to know rules to enhance privacy.

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

  CMS-OFCCP is currently in Operations & Maintenance Phase.

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

  Not applicable. Security was built into the design of the system.

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?

OFCCP has determined that the safeguards and controls for this moderate system adequately protect the information. OFCCP 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

Shiaolin Tsai Digitally signed by Shiaolin Tsai
Date: 2023.07.11 13:07:46
-04'00'

Shiaolin (Shirley) Tsai
CMS OFCCP System Owner

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
- ☐ 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)

- [x] Mailing address (e.g., P.O. Box)
- [x] Personal e-mail address
- [x] Business address
- [x] Business phone number (e.g., phone, fax, cell)
- [x] 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?

  No. Information is obtained as part of investigations to resolve complaints of discrimination filed by individuals under Executive Order 11246, as amended; the Veteran Era Veterans' Readjustment Assistance Act of 1974, amended, 38 U.S.C. 4212; and section 503 of the Rehabilitation Act of 1973, as amended, 29 U.S.C.793.

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

  N/A- see statement above