PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

COLLABORATION MANAGEMENT AND METRIC SOLUTION - CM-MS

2. DOD COMPONENT NAME:

Defense Information Systems Agency

DISA SD2

3. PIA APPROVAL DATE:

8/10/2021

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)*

- ☐ From members of the general public
- ☒ From Federal employees
- ☐ from both members of the general public and Federal employees
- ☐ Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one.)*

- ☒ New DoD Information System
- ☐ New Electronic Collection
- ☐ Existing DoD Information System
- ☐ Existing Electronic Collection
- ☐ Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

CM-MS is a general support system (GSS) supported by Salesforce SaaS. Salesforce is a Customer Relationship Management (CRM) solution.This SaaS is instantiated via the Salesforce Org being stood up. It will eventually be utilized to support multiple applications using Salesforce/Tableau. The initial application of the SaaS capability initially being stood up called the Business Intelligence (BI) prototype which will serve as an initial 'Proof of Concept' of Salesforce's capabilities. BI prototype will demonstrate Salesforce's CRM and analytics capabilities by processing a subset of data sourced from CMIS on behalf of the Workforce Services Directorate (WSD). Manual WSD reports utilized today will be recreated via the Salesforce/Tableau functionality in a mechanized manner. A limited number of PII (e.g. ID number, Name, Location) fields will be loaded into Salesforce in order to recreate the existing reports.

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

For Salesforce CM-MS, and the generic SaaS capability, there is storage of DoD Id numbers. The initial application, (BI prototype), of this GSS will utilize PII as part of its mission, in order to showcase Salesforce capabilities for DISA WSD and SD2 by recreating existing capabilities in this new environment. A limited number of PII fields (e.g. ID number, Name, Location) will be loaded into Salesforce in order to recreate the existing reports.

e. Do individuals have the opportunity to object to the collection of their PII? ☐ Yes ☒ No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

For the generic CM-MS capability 'No'. Within the BI prototype 'No,' the tool is being used to recreate existing capabilities and the management of PII collected and sourced is internal to HR/ DISA WSD.

f. Do individuals have the opportunity to consent to the specific uses of their PII? ☐ Yes ☒ No

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

For CM-MS capability 'No'. For BI prototype 'No', the tool is being used to recreate existing reporting capabilities and PII collection is internal to HR/WSD.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and provide the actual wording.)*

- ☐ Privacy Act Statement
- ☒ Privacy Advisory
- ☐ Not Applicable

Definition of Personal Information:
Personal information means recorded information about an identifiable individual, including the individual's name, telephone number, email address, and working company (and/or contract). The ATIPP Act outlines several examples of personal information.
Collecting Personal Information:
The only identifiable personal information collected by this form is information given voluntarily. Any personal information provided through this form is considered non-sensitive PII. This information is collected in compliance with the ATIPP Act and will only be used by authorized staff to establish individual login credentials.
The refusal to provide personal information through this website will result in the restriction of access to government controlled or privately held pages.
Security:
Users shall not attempt to bypass their permissions level. Users shall not share password or login credentials.
Users assert that all information provided via this form is correct.
The use of an authorized account by an individual whose information does not align with the information provided on this form is prohibited.

h. With whom will the PII be shared through data/system exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

☒ Within the DoD Component	Specify.	DISA
☐ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	
☐ Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	
☐ State and Local Agencies	Specify.	
☐ Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*	Specify.	
☐ Other *(e.g., commercial providers, colleges).*	Specify.	

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

☒ Individuals	☐ Databases
☒ Existing DoD Information Systems	☐ Commercial Systems
☐ Other Federal Information Systems	

a. For CM-MS - individuals aka. users
b. For BI prototype - Employee PII is sourced from DISA CMIS solution.

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

☐ E-mail	☐ Official Form (*Enter Form Number(s) in the box below)*
☐ In-Person Contact	☐ Paper
☐ Fax	☐ Telephone Interview
☒ Information Sharing - System to System	☒ Website/E-Form
☐ Other *(If Other, enter the information in the box below)*	

a. For CM-MS, website/e-form.
b. For BI prototype data is extracted from CMIS via ad-hoc report and loaded into Salesforce community.

k. Does this DoD Information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information must be consistent.

☒ Yes ☐ No

If "Yes," enter SORN System Identifier K890.27

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority. N/A

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

No retention required. This system is a prototype and not fully funded. Reports on job losses, gains and offers being generated by manually pulling data from CMIS and loading into SalesForce to generate reports. WSD currently manually generates these reports. Information is duplicative because it is not original to the CMMS.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply).

(a) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) If direct or indirect authority does not exist, DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component must be identified.

10 U.S.C. Chapter 8-Defense Agencies and Department of Defense Field Activities; DoD Directive (DoDD) 5105.19, Defense Information Systems Agency (DISA); DoD Directive 1000.25, DoD Personnel Identity Protection (PIP) Program; DoD Enterprise User Data Management Plan for Persons and Personas; and DoD Global Information Grid 2.0 Concept of Operations (GIG 2.0 CONOPS); DoDI 5200.46-DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC) and DoDI 8520.03-Identity Authentication for Information Systems.

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (OMB) Control Number?

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information. This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ Yes ☒ No ☐ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

OMB approval is not required in accordance with Section 8.b.11 of Enclosure 3 of DoD Manual 8910.01- Volume 2.