PRIVACY IMPACT ASSESSMENT (PIA)

For the

CRM - MS DYNAMIC CUSTOMER RELATIONSHIP MANAGEMENT (TOOL)

FORSCOM [AFSGS], SGS-KM

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☒ (2) Yes, from Federal personnel* and/or Federal contractors.

☐ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

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

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- ☒ **Yes, DITPR** Enter DITPR System Identification Number: 15306 DA206207
- ☐ **Yes, SIPRNET** Enter SIPRNET Identification Number:
- ☐ **No**

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- ☐ **Yes**
- ☒ **No**

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. 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 should be consistent.

- ☒ **Yes**
- ☐ **No**

If "Yes," enter Privacy Act SORN Identifier

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an 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**

Enter OMB Control Number

Enter Expiration Date

☒ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) 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) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect 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) 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 should be identified.

Defense Production Act of 1950, E.O. 11179 dated September 22, 1964, as amended by E.O. 12148 dated July 20, 1979, 5 U.S.C. 301; the Federal Records Act, 44 U.S.C. 3101; Executive Order 9397; AR 25-1 Army Information Management; AR 380-19, Information Systems Security.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

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

Microsoft Dynamics CRM is a server-client application, which, like Share Point, is primarily an IIS-based web application which also supports extensive web services interfaces. Clients access Dynamics CRM either by using Microsoft Internet Explorer 6 or later web browser or by a thick client plug-in to Microsoft Outlook. For the purposes of FORSCOM's application, CRM will plug into outlook. CRM enables a host of bolt-on modules that will support various processes within the Command both administrative and operational. Primarily, CRM will host an application called Task Management Tool or TMT. TMT will replace the antiquated E-Tasker system used internally by the command as well as provide a new automated procedure to the processing of Awards and Decorations, Evaluations, and OPORD/FRAGO tasking originating from G3.

The CRM provisioned SharePoint site collection does not directly collect any PII information nor is it a source for collection of PII. All forms and documents submitted through the system are covered and contained in other systems of records.

The SharePoint site collection requires CAC authentication, and therefore cannot be used by a user routed through fce.forscom.army.mil or from the NASE at fcportal.forscom.army.mil unless they have first authenticated. Permissions to documents are managed by the Dynamics CRM application. The CRM application requires CAC authentication and like SharePoint is located behind the reverse proxy. CRM grants users permissions by role and team. Team permissions are managed locally in the directorate office by the respective executive officer (XO) and SGS-KM.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

Due to the level of safeguarding , the risk to the individual's privacy is minimal. Access to documents containing PII is based on a need to know only basis and is based on permissions and roles. System administrators control access to restricted information using these managed permissions. Access to this data collection instrument is only possible if the individual has an account and is only accessed with a CAC Card.

CRM creates a new sub-site within SharePoint with individual permissions for each activity record. This further mitigates the risk of users without read permissions to view PII files.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. Depending on the CRM activity that is created and assigned to a user or group. This will give permissions to different entities that need to review the PII information

☐ **Other DoD Components.**

Specify.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

☐ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

☐ **Other** (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

☐ **Yes** ☒ **No**

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

(2) If "No," state the reason why individuals cannot object.

PII in this SharePoint site collection is not collected directly from the user, thus they cannot object. Documents such as awards and evaluations that contain PII are stored in SharePoint site collection directory created by the CRM application.

j. 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.

PII in this SharePoint site collection is not collected directly from the user, thus they cannot object. Documents such as awards and evaluations that contain PII are stored in a SharePoint site collection directory created by the CRM application.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☐ **Privacy Act Statement** ☒ **Privacy Advisory**

☐ **Other** ☐ **None**

Describe each applicable format.

DoD Disclaimer
Use of this or any other DoD interest computer system constitutes consent to monitoring at all times. This is a DoD interest computer system. All DoD interest computer systems and related equipment are intended for the communication, transmission, processing, and storage of official U.S Government or other authorized information only. All DoD interest computer systems are subject to monitoring at all times to ensure proper function of equipment and systems including security devices and systems, to prevent unauthorized use and violations of statutes and security regulations, to deter criminal activity, and for other similar purposes. Any user of a DoD interest computer system should be aware that any information placed in the system is subject to monitoring and is not subject to any expectation of privacy

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.