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:

Enterprise Mission Assurance Support Service (eMASS)

2. DOD COMPONENT NAME:

Defense Information Systems Agency

ID31

3. PIA APPROVAL DATE:

01/29/24

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.

eMASS is a web-based application providing automation for comprehensive, fully integrated cybersecurity management, including controls management, workflow automation, continuous monitoring, and dashboard reporting to support assessments, authorizations, and certification processes for information systems and organizations. Data collection/use includes federal employees, contractors, and defense industrial base.

eMASS utilizes a role-based access model and current DoD/Federal Government authentication requirements for users. This includes PKI/ certificate information (e.g., CAC/PIV) or identifier from an Identify Provider (Single Sign-On (SSO)). Information collection for users is specific to individuals that directly register for an eMASS user account.

For CMMC eMASS, data is collected to fulfill the CMMC mission and limited to minimally required information for the DoD's CMMC Repository requirements. This includes data provided by the CMMC Cyber Accreditation Body (e.g., accreditation status of Certified Third-Party Assessor Organizations (C3PAOs), approved/licensed assessors, and C3PAOs/organizations approved as CMMC training/publishing partners). The types of PII collected are as follows: Name(s), DoD ID Number, Other ID Number, Security Information, Position/Title, Official Duty Telephone Phone, Work E-mail Address, Official Duty Address.

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)*

PII is collected for user account creation and contact information. The intended use of PII is to provide automated email notifications, allow eMASS administrators to manage user access to the eMASS application, determine the specific eMASS roles/permissions needed for each user, and contact personnel for an emergency or if immediate action is required to protect DoD information systems.

For CMMC eMASS, the information provided by the CMMC Cyber Accreditation Body is intended to provide DoD with visibility into accredited C3PAOs, certified assessors, approved training partners, and approved publishing partners to ensure that assessments/ certifications that are being conducted against the Defense Industrial Base are meeting established requirements. This limited collection is also intended to digitally fulfill the transfer of requisite information from the CMMC ecosystem to the Federal Government to reduce paperwork.

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.

The collected PII is required to create a unique account for each user that needs access to eMASS. Without the collected information, eMASS administrators would not be able to manage user accounts within the eMASS application. Individuals may object to the collection of

PII by not providing the requested information, however this information is required to gain access to the eMASS application. Users opt-in to participate as part of the CMMC Ecosystem (e.g., C3PAO, Assessor, etc.) collected by the CMMC Cyber Accreditation Body -- eMASS receives minimally required information from the CMMC Cyber Accreditation Body for the DoD's CMMC requirements.

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.

Prior to accessing eMASS, the standard DoD Warning Banner for collection of information is displayed. Users can also review the Security Notice, Privacy Advisory, and Accessibility Statement. Individuals can withhold their consent by not providing the requested information, however this information is required to register for an account.

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

Users can access the eMASS Privacy Advisory via a hyperlink in the footer of all eMASS webpages, including when first accessing the application. The eMASS Privacy Advisory displayed to individuals is: "TThis is a DoD interest system. This system collects information about users protected under the Privacy Act of 1974. This information includes the email address, phone number, and contact information of individuals who are responsible for handling emergencies for computer systems and networks. This information is used to provide email notifications and contact information of personnel for an emergency or if immediate action is required to protect information systems."

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.	All DoD Component, Agency, Organization, Army, DARPA, DAU, DCAA, DCMA, DECA, DFAS, DHA, DHRA, DIB, DIU, DLA, DMA, DMEA, DoD IG, DoDEA, DPAA, DSCA, DSS, DTIC, DTRA, DTSA, HPCMP, JIDO, Joint, JSP, MDA, Navy, NGB, OSD/DoD CIO, PFPA, SD, SOCOM, Air Force, USTRANSCOM, WHCA, Space Force, CYBERCOM, SPACECOM, USCAAF, SDA, OUSD(I&S), OMC, OLDCC, Marine Corps, CDAO
☒ Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	Coast Guard, NASA, Department of Commerce, Department of Veterans Affairs
☐ 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.	CMMC Cyber Accreditation Body (for CMMC AB/ Ecosystem information), Defense Industrial Base/ Commercial Providers/Contractors.

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

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)*

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 K890.16 DoD

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. DAA-GRS-2013-0005-0003; DAA-0371-2021-0001-0001

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

(3) Retention Instructions.

For DAA-GRS-2013-0005-0003, the retention period is destroy 5 years after the project/activity/transaction is completed or superseded, or the associated system is terminated, or the associated data is migrated to a successor system, but longer retention is authorized if required for business use. For DAA-0371-2021-0001-0001, the cutoff is annually by calendar year. Retention period is destroy 25 years after cutoff.

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.

The following authority allows eMASS to collect the data:
- 5.U.S.C 301, Departmental Regulation
- DoD Directive 5105.19, Defense Information Systems Agency
- DoDI 8510.01, Risk Management Framework for DoD Information Technology

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.

eMASS PMO is coordinating with DoD WHS and OMB to acquire an OMB Contract Number.