

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

3. PIA APPROVAL DATE:

10/13/20

ID31

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: (Check one. Note: foreign nationals are included in general public.)

- | | |
|---|---|
| <input type="checkbox"/> From members of the general public | <input checked="" type="checkbox"/> From Federal employees and/or Federal contractors |
| <input type="checkbox"/> From both members of the general public and Federal employees and/or Federal contractors | <input type="checkbox"/> Not Collected (if checked proceed to Section 4) |

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

- | | |
|--|---|
| <input type="checkbox"/> New DoD Information System | <input type="checkbox"/> New Electronic Collection |
| <input checked="" type="checkbox"/> Existing DoD Information System | <input type="checkbox"/> Existing Electronic Collection |
| <input type="checkbox"/> 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 Government off-the-shelf (GOTS), software as a service (SaaS) capability that automates a broad range of processes for comprehensive, fully integrated cybersecurity management, including dashboard reporting, workflow automation, and continuous monitoring supporting Risk Management Framework (RMF) for Assessment and Authorization (A&A).

eMASS utilizes a role-based access model combined with PKI authentication. The following information is collected for each individual that registers and is approved for an eMASS account: First Name, Last Name, Organization, Business Phone, Business Email, Official Duty Address. The user's PKI certificate is also captured and stored in the database as eMASS is PKI/CAC-enabled.

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 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.

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.

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 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 gain access to the eMASS application.

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.)

- | | | |
|--|--|---|
| <input type="checkbox"/> Privacy Act Statement | <input checked="" type="checkbox"/> Privacy Advisory | <input type="checkbox"/> 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: "This is a DoD interest system. This system collects information about users protected under the Privacy Act of 1974. This information includes the business contact information for individuals who are responsible for handling emergencies for computer systems and networks. This information is used to contact personnel for an emergency or if immediate action is required to protect information systems."

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

- Within the DoD Component Specify. DISA
Army, DAU, DCAA, DCMA, DECA, DFAS, DHA, DHRA, DIB, DLA, DMA, DoD IG, DoDEA, DPAA, DSCA, DSS,
- Other DoD Components Specify. DTIC, DTRA, DTSA, HPCMP, JIDO, JS, JSP, MDA, Navy, NGB, OSD, PFPA, RACE, SOCOM, USAF, USTRANSCOM, WHCA, WHS
- Other Federal Agencies 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.

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

It is collected from individuals request eMASS account.

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)
- Face-to-Face Contact Paper
- Fax Telephone Interview
- Information Sharing - System to System Website/E-Form
- Other (If Other, enter the information in the box below)

Users must input the requested information when registering for an eMASS account.

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

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

(3) Retention Instructions.

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 statute 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, Department of Defense Information Assurance Certification and Accreditation Process (DIACAP).

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.