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:

Veterinary Services Information Management System (VSIMS)

2. DOD COMPONENT NAME:

Defense Health Agency

Program Executive Office (PEO) Medical Systems

3. PIA APPROVAL DATE:

01/27/23

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
X 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
X 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.

The Veterinary Service Information Management System (VSIMS) is a tri-Service application used to collect, store, and report information supporting Department of Defense (DoD) level missions for Veterinary Service Public Health. The Veterinary Service Public Health has two main missions: (1) Animal Medicine. Animal Health topics such as military working dogs protection during deployment, zoonotic diseases such as rabies, and animal diseases of military interest; and (2) Food Protection and Public Health Sanitation. The Food Protection program provides guidance regarding issues concerning food quality and wholesomeness which impact the health of DoD personnel.

The VSIMS is comprised of custom built modules that manage workflows, including but not limited to, audits of commercial food establishments, sanitation inspections of military food and animal housing facilities, hazardous recalls of DoD-owned subsistence, lifecycle food protection for operational rations, food and water risk assessments across the DoD supporting short term missions or exercises, laboratory food sample submission and results, veterinary equipment data, and animal bite-scratch report tracking. The data in workflows is not related to an individual and does not contain PII. This system also serves as a controlled source of information needed by Veterinary Unit personnel to perform assigned duties and other tasks, such as information from the Worldwide Directory of Sanitarily Approved Food Establishments for Armed Forces Procurement, food/non-prescription drug recalls, information on operational rations, Food & Water Risk Assessments, etc.

Personally Identifiable Information (PII) collected by VSIMS is strictly used for user identification and authentication purposes only, and is limited to the following: the user's DoD ID number which is stored in the user's profile and used for authentication prior to allowing access to a session; the user's name and rank where applicable, which is used for identification; and the user's phone number (when entered or requested to be entered by the user) which is stored in the user's profile and used by the commercial audit module.

The categories of individuals with PII and records in this system include: Department of Defense military personnel Army, Navy, and Air Force (active and reserve component); Department of Defense civilians; Non-Appropriated Fund (NAF) employees; and members of the public (Foreign Nationals only). The Foreign Nationals are individuals employed by the veterinary unit, which is either a Public Health Activity or Regional Public Health Command, located in Europe, Japan, and Korea.

VSIMS is owned and managed by the Solution Delivery Division (SDD).

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)*

1) PII is collected from existing DoD Information Systems as part of the account request process prior to gaining access to VSIMS, and is needed for controlling access to the system thereafter. Once the account is created, PII is never collected again.
2) Once a user is authenticated by Identity Authentication Services (iAS), the DoD ID number is passed to VSIMS for comparison with the

DoD ID number stored for that user in the their profile. An exact match is required before the user is granted access. Name and rank are collected for identification and access controls within the system, and official telephone number is used within VSIMS in support of the commercial audit module. This is the only PII stored in and used by the VSIMS.
3) The following provides the lifecycle management of the PII: PII is manually entered in the system; utilized for identification and authentication throughout the user's tenure; archived when the user account is terminated; and stored in archive until no longer required for administrative use.

e. Do individuals have the opportunity to object to the collection of their PII? Yes x 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.

Individuals do not have the opportunity to object to the collection of their PII because VSIMS is not the initial point of collection.

f. Do individuals have the opportunity to consent to the specific uses of their PII? Yes x 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.

Individuals do not have the opportunity to consent to the specific uses of their PII because VSIMS is not the initial point of collection.

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 | x Not Applicable

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)*

x	Within the DoD Component	Specify.	Authorized VSIMS Users Within the Solution Delivery Division (SDD); DHA Public Health Division
x	Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	Authorized VSIMS Users Within the Departments of the Army, Navy, and Air Force
	Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	
	State and Local Agencies	Specify.	

x	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.	PII is shared with VSIMS support personnel under the contract with Malama LLC, which includes the following applicable FAR Privacy Clauses: FAR Clause 52.239-1, Privacy or Security Safeguards: "(a) The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government. (b) To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases. (c) If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party." and FAR Clause 52.224-3, Privacy Training (JAN 2017): "...(b) The Contractor shall ensure that initial privacy training, and annual privacy training thereafter, is completed by contractor employees who- (1) Have access to a system of records; (2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information on behalf of an agency; or (3) Design, develop, maintain, or operate a system of records (see also FAR subpart 24.3 and 39.105). (c) (1) "Privacy training shall address the key elements necessary for ensuring the safeguarding of personally identifiable information or a system of records. The training shall be role-based, provide foundational as well as more advanced levels of training, and have measures in place to test the knowledge level of users. At a minimum, the privacy training shall cover-(i) The provisions of the Privacy Act of 1974 (5 U.S.C. 552a), including penalties for violations of the Act; (ii) The appropriate handling and safeguarding of personally identifiable information; (iii) The authorized and official use of a system of records or any other personally identifiable information; (iv) The restriction on the use of unauthorized equipment to create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise access personally identifiable information; (v) The prohibition against the unauthorized use of a system of records or unauthorized disclosure, access, handling, or use of personally identifiable information; and (vi) The procedures to be followed in the event of a suspected or confirmed breach of a system of records or the unauthorized disclosure, access, handling, or use of personally identifiable information (see OMB guidance for Preparing for and Responding to a Breach of Personally Identifiable Information). (2) Completion of an agency-developed or agency-conducted training course shall be deemed to satisfy these elements. (d) The Contractor shall maintain and, upon request, provide documentation of completion of privacy training to the Contracting Officer...."
	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
x	Existing DoD Information Systems		Commercial Systems
	Other Federal Information Systems		

- US Army Medical Center of Excellence (MEDCoE) class rosters obtained from the Army Training Requirements and Resource System (ATRRS).
- The Global Veterinary Medical Practice (GVMP) provides a monthly roster of NAF employees.
- Foreign National's information (name only) is verified via email with their employing Public Health units.
- Air Force users' information is verified/confirmed via a Air Force Medical Support Agency (AFMSA) POC.
- Navy users information is verified/confirmed by the user directly via phone or email. Note: There are only 40 Navy users.

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

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

Information Sharing - System to System: Identity Authentication Services (iAS)
The ATRRS generates a class roster for the MEDCoE and manually emails it to the VSIMS Administrators for the purpose of VSIMS account creation.

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.

x Yes No

If "Yes," enter SORN System Identifier DMDC 02

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. Unscheduled

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

(3) Retention Instructions.

Unscheduled - Permanent. Treat system and/or records maintained in the system as permanent until a NARA approved schedule and disposition authority has been applied.

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.

5 U.S.C. App. 3, Inspector General Act of 1978; 5 U.S.C. Chapter 90, Federal Long-Term Care Insurance; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. Chapter 53, Miscellaneous Rights and Benefits; 10 U.S.C. Chapter 54, Commissary and Exchange Benefits; 10 U.S.C. Chapter 58, Benefits and Services for Members being Separated or Recently Separated; 10 U.S.C. Chapter 75, Deceased Personnel; 10 U.S.C. 2358, Research and Development Projects; 10 U.S.C. 987, Terms of Consumer Credit Extended to Members and Dependents; 20 U.S.C. 1070h, Scholarships for Veteran's Dependents; 31 U.S.C. 3512(c), Executive Agency Accounting and Other Financial Management Reports and Plan; 38 U.S.C. Chapter 19, Subchapter III, Service members' Group Life Insurance; 42 U.S.C. 18001 note, Patient Protection and Affordable Care Act (Pub. L. 111-148); 42 U.S.C. 1973ff, Federal Responsibilities; 50 U.S.C. Chapter 23, Internal Security; 50 U.S.C. Chapter 50, Servicemembers Civil Relief Act; DoD Directive 1000.04, Federal Voting Assistance Program (FVAP); DoD Directive 1000.25, DoD Personnel Identity Protection (PIP) Program; DoD Instruction 1015.9, Professional United States Scouting Organization Operations at United States Military Installations Located Overseas; DoD Instruction 1100.13, Surveys of DoD Personnel; DoD Instruction 1241.03 TRICARE Retired Reserve (TRS) Program; DoD Instruction 1241.04, TRICARE Reserve Select (TRS) Program; DoD Instruction 1336.05, Automated Extract of Active Duty Military Personnel Records; DoD Instruction 1341.2, Defense Enrollment Eligibility Reporting System (DEERS) Procedures; DoD Manual 1341.02, DoD Identity Management DoD Self-Service (DS) Logon Program and Credential; DoD Instruction 3001.02, Personnel Accountability in Conjunction with Natural or Manmade Disasters; Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors; DoD Instruction 7730.54, Reserve Components Common Personnel Data System (RCCPDS); 38 CFR 9.20, Traumatic injury protection; and E.O. 9397 (SSN), as amended.

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 [x] 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.

In accordance with DoDM 8910.01, Volume 2, VSIMS does not require OMB approval per Enclosure 3, Section 8, subsection a(1): "Public Information Collections Addressed to Nine or Fewer Persons," and per Enclosure 3, Section 8, subsection b(10).