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:

Consolidated System Tracking And Reporting (CSTAR)

2. DOD COMPONENT NAME:

Defense Health Agency

3. PIA APPROVAL DATE:

07/07/2026

Program Executive Office (PEO) Medical Systems (J6)

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.

Consolidated System Tracking and Reporting (CSTAR) is a cybersecurity workflow application that centralizes project information and allows resources to track systems through each step of the Risk Management Framework (RMF) lifecycle.

CSTAR's primary purpose is to track systems through the RMF lifecycle. To facilitate this, CSTAR collects the following types of PII: individual names, official government email addresses, and official government phone numbers. This information is collected to create a definitive list of Points of Contact (POCs) for the systems being tracked.

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 to identify and maintain an accurate record of the key personnel (e.g., Program Managers, ISSMs, ISSOs, Engineers) responsible for the systems undergoing the RMF process within CSTAR.

Intended Use: The intended use of the PII is for mission-related communication and administrative use. It allows cybersecurity stakeholders to contact the correct POCs regarding RMF taskings, security controls, and system status. The PII is used to generate contact lists and facilitate official government business.

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.

CSTAR is not the source system where the initial collection occurs.

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.

CSTAR is not the source system where the initial collection occurs.

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

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.	DHA
☒ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	Army, Air Force, Navy, and Coast Guard
☐ 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.	Contractor personnel comprising the CSTAR development, administration, and support team have access to the PII (official business contact information) solely for the purpose of system maintenance, troubleshooting, and user support. Data is not exchanged with, or exported to, any contractor's corporate network; all access occurs securely within the government-controlled MED365 boundary. Contractor access is safeguarded by standard Defense Federal Acquisition Regulation Supplement (DFARS) clauses (e.g., 252.204-7012), mandatory non-disclosure agreements (NDAs), and the requirement to hold appropriate personnel security clearances. Furthermore, all contractor personnel are required to complete annual DoD Privacy Act and Cybersecurity training prior to obtaining administrative access.
☐ 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

Information imported manually from existing authoritative DoD systems (e.g., eMASS system records).

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)*

Manually data imports (e.g., CSV uploads) from eMASS.

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

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.

CSTAR is not a privacy act system of records, where a group of records is being maintained and retrieved by an individual's name, number or unique identifier.

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.

Mission Schedules:
- GRS 3.2, item 010 (DAA-GRS-2013-0006-0001)
Other Schedules:
- System Access Records: GRS 3.2, item 030 (DAA-GRS-2013-0006-0003),
- Data Administration and Documentation: GRS 3.1, item 051 (DAA-GRS-2013-0005-0003)

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

(3) Retention Instructions.

Mission Schedules:
FILE NUMBER: 1606-05
FILE TITLE: Systems and Data Security Records
DISPOSITION: Temporary. Cut off after system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system. Destroy 1 year after cutoff.

Other Schedules:
FILE NUMBER: 1601-02
FILE TITLE: System Access Records - Systems not requiring Special Accountability for Access
DISPOSITION: Temporary. Cut off and destroy when business use ceases.

FILE NUMBER: 1601-12
FILE TITLE: Data Administration and Documentation - Temporary Systems
DISPOSITION: Temporary. Cut off 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. Destroy 5 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.

10 U.S.C. 113, Secretary of Defense; DoW Instruction 8510.01, Risk Management Framework for DoD Systems; DoW Instruction 8500.01, Cybersecurity; and the Federal Information Security Modernization Act of 2014 (FISMA).

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.

An OMB Control Number is not required. CSTAR exclusively collects official business contact information (Name, Official Email, Official Phone) from internal DoD personnel and DoD contractors acting within the scope of their official duties to facilitate internal RMF workflows.
In accordance with DoW Manual 8910.01, Volume 2, OMB clearance and an associated Control Number are only required when conducting "information collections from the public." Federal employees and U.S. Government contractors acting within the scope of their contracts are explicitly excluded from the definition of the "public" for the purposes of the Paperwork Reduction Act.
Specific: DoW Manual 8910.01, Volume 2, does not apply to CSTAR reference, "....b.Does not apply to: (1)Component internal information collections that do not collect information from members of the public...." page 2, paragraph b. (1).