

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:

DevSecOps Community Cloud (DSOCC)

2. DOD COMPONENT NAME:

Defense Health Agency

3. PIA APPROVAL DATE:

03/05/2026

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.

The DevSecOps Community Cloud (DSOCC) mission objective is to provide a scalable cloud or on-premises platform to develop, run, and manage applications while relieving application teams of the complexity of systems administration and infrastructure maintenance. DevSecOps Community Cloud, which is GIG connected, provides a virtualized container environment that streamlines application development allowing for the continuous integration and delivery to improve application functionality and security in support of Defense Health Agency (DHA) military healthcare delivery operations. The Rancher Platform consists of a control plane and worker nodes with containerized storage architecture within a dedicated network offering a robust suite of Development Operations (DevOps) tools, container image and code repositories, and container security. The DevSecOps Community Cloud currently supports eighteen customers providing a wide spectrum of services across the DHA.

Personally Identifiable Information (PII) may include numerous types of PII including employee and beneficiary contact information, military information, demographic information, Social Security Number (SSN), and Protected Health Information (PHI).

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)

DSOCC is Development Cloud Environment provider for the DHA medical community users, and as such they may store PII on within the the Container platform and Gitlab specifically in support of their clinical and business workflows within the Government Cloud Environment. PII/PHI is not collected by DSOCC PII/PHI maybe part of the POR that is utilizing the DSOCC platform. The POR will have a separate PIA that covers there PII/PHI within there ATO boundry.

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.

Individuals do not have the opportunity to object to the collection of their PII /PHI because this system is not the initial point of collection; however, the source system may provide the individual the opportunity to object to the collection.

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.

Individuals do not have the opportunity to object to the collection of their PII /PHI because this system is not the initial point of collection; however, the source system may provide the individual the opportunity to object to the 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 Not Applicable

This system is not the initial collection point for the PII. The PII is obtained from an existing DoD information system or electronic collection, therefore no Privacy Act Statement or Privacy Advisory is required.

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)

- | | | |
|---|----------|--|
| <input checked="" type="checkbox"/> Within the DoD Component | Specify. | <input type="text" value="DHA"/> |
| <input checked="" type="checkbox"/> Other DoD Components (i.e. Army, Navy, Air Force) | Specify. | <input type="text" value="DHMS, Navy, Army, Air Force, VA"/> |
| <input type="checkbox"/> Other Federal Agencies (i.e. Veteran's Affairs, Energy, State) | Specify. | <input type="text"/> |
| <input type="checkbox"/> State and Local Agencies | Specify. | <input type="text"/> |

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.)

Various contractors supporting DHA provide system administration for DevSecOps Community Cloud (DSOCC) and adhere to the following safeguards for PII as required by their respective contracts:

Specify. When a contractor, including any subcontractor, is authorized access to Personally Identifiable Information (PII), the contractor shall complete annual PII training requirements and comply with all privacy protections under the Privacy Act (Clause 52.224-1 and 52.224-2). The contractor shall safeguard PHI/PII from theft, loss, and compromise, and shall safeguard, transmit and dispose of PHI/PII in accordance with the latest DHA and DoD policies and the contractor's HIPAA Business Associate Agreement (BAA). The contractor shall mark all developed documentation containing PII information accordingly in either the header or footer of the document: "FOUO – Privacy Sensitive. Any misuse or unauthorized disclosure may result in both criminal and civil penalties." Any unauthorized disclosure of privacy sensitive information through negligence or misconduct can lead to task order removal or task order termination depending on the severity of the disclosure. Upon discovery of a PII breach, the contractor shall immediately notify the Contracting Officer and contracting officer representative (COR). This list of contractors includes:
Spinvi, Accelera Solutions, Core4ce, KSH, NSSPlus, BEAT, DXC, SpinSys, MITRE

- 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)

- | | |
|---|---|
| <input type="checkbox"/> Individuals | <input checked="" type="checkbox"/> Databases |
| <input checked="" type="checkbox"/> Existing DoD Information Systems | <input type="checkbox"/> Commercial Systems |
| <input checked="" type="checkbox"/> Other Federal Information Systems | |

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

- | | |
|---|--|
| <input type="checkbox"/> E-mail | <input type="checkbox"/> Official Form (Enter Form Number(s) in the box below) |
| <input type="checkbox"/> In-Person Contact | <input type="checkbox"/> Paper |
| <input type="checkbox"/> Fax | <input type="checkbox"/> Telephone Interview |
| <input checked="" type="checkbox"/> Information Sharing - System to System | <input type="checkbox"/> Website/E-Form |
| <input type="checkbox"/> 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

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or <http://dpclid.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.

Mission Records: GRS 3.1, item 011 (DAA-GRS- 2013-0005- 0007)

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 Records:
FILE NUMBER: 1601-01
FILE TITLE: System Development Records
DISPOSITION: Temporary. Cut off after system is superseded by a new iteration, or is terminated, defunded, or when no longer needed for administrative, legal, audit, or other operational purposes. Destroy 5 years 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 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.

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.

The information collected in this system and is not considered a public information collection in accordance with DoDM 8910.01, V2, Encl 3, paragraph 8b(5).