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:

SD DevSecOps

2. DOD COMPONENT NAME:

Defense Information Systems Agency

3. PIA APPROVAL DATE:

3/17/2022

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 SD DevSecOps system provides tools to check, scan and validate mission partner containerized applications using STIG Automation Compliance as Code (CaC) files. This provides mission partners in the field, the ability to improve their DevSecOps security posture. Mission partners can create an ID, based upon their email address to download and utilize these STIG CaC files. This system also allows content contributors (vendors) to create CaC files based upon STIGs that they have created and submit them to the SD DevSecOps system to perform a Quality Assurance (QA) analysis through the SD DevSecOps QA pipeline. Once approved, these files can be used throughout the DoD for compliance scanning. These scans follow DoD STIG guidance, for security posture reporting of mission owners' DevSecOps environments. Contributors are required to provide an email and password to create accounts and access this system. This information is stored in AWS on a FIPS compliant encrypted EBS instance. Multi Factor Authentication (MFA) will be used for those content contributors who will push data to the system. Includes, Name, Personal E-mail Address, and Work E-mail 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)*

SD DevSecOps collects email addresses and passwords as authentication to utilize a GitLab and Dashboard system. The data is only intended to allow users access to download CaC files and guarantee ID uniqueness.

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.

A unique ID is required to be granted access to the CaC files in the form of an email. The user does however have the ability to provide any email address as a valid ID to obtain access. Users can choose not to use the system and thus object to the collection of PII.

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.

Users have the ability to use any email address they wish as long as its unique to the DevSecOps system. The PII collected is required for the user to log into the system and its components. Users have a choice of being able to use the system.

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

Solicitation of a unique email ID is authorized under the Privacy Act of 1974 section 3(e)(3). Your email is a unique identifier and disclosure is necessary in some circumstances to assure a unique ID and account.
We will only share the email information you give us with another government agency if your inquiry relates to that agency, or as otherwise required by law. We do not share information you give us with any private organizations. The SD DevSecOps CaC system never collects information for commercial marketing. While you must provide an e-mail address for a response other than those generated automatically in response to questions, comments, or feedback that you may submit, we recommend that you NOT include any other personal information, especially Social Security numbers. The Social Security Administration offers additional guidance on sharing your Social Security number.
This government computer system uses software programs to create summary statistics, which are used for such purposes as assessing what information is of most and least interest, determining technical design specifications, and identifying system performance or problem areas.
For site management, information is collected for analytical and statistical purposes. This government computer system uses software programs to create summary statistics which are used for such purposes as assessing what information is of most and least interest, determining technical design specifications, and identifying system performance or problem areas.
For site security purposes and to ensure that this service remains available to all users, this government computer system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.
Your interaction with this system is not anonymous. By using this system you are consenting to the monitoring of your activity. Raw data logs will only be used to identify individual users and their usage habits for authorized law enforcement investigations, national security purposes, or investigation of the SD DevSecOps CaC performance issues. These logs are used for no other purposes and are scheduled for regular destruction in accordance with National Archives and Records Administration General Schedule 20. Email IDs not used for over a year will be destroyed in accordance to NARA General Schedule 20.
Unauthorized attempts to deny service, upload information, or change information from this site are strictly prohibited and may be punishable under Title 18 of the U.S. Code to include the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act.
If you have any questions or comments about the information presented here, please submit feedback to disa.meade.sd.mbx.devsecops-mailbox@mail.mil

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.
☐	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.
☐	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		

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 K890.15

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. GRS 3.2 #30. DAA-GRS-2013-0006-0003

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

(3) Retention Instructions.

Raw data logs will only be used to identify individual users and their usage habits for authorized law enforcement investigations, national security purposes, or investigation of SD DevSecOps CaC performance issues. These logs are used for no other purposes and are scheduled for regular destruction in accordance with National Archives and Records Administration GENERAL RECORDS SCHEDULE 3.2: Information Systems Security Records. IDs that have not been utilized for a year or more will be destroyed according to GRS 3.2 #30.

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. Chapter 8-Defense Agencies and Department of Defense Field Activities; DoD Directive (DoDD) 5105.19, Defense Information Systems Agency (DISA); DoD Directive 1000.25, DoD Personnel Identity Protection (PIP) Program; DoD Enterprise User Data Management Plan for Persons and Personas; DoDI 5200.46-DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC) and DoDI 8520.03-Identity Authentication for Information Systems.

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.