

## 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:**

C2 Software Factory (C2SF)

**2. DOD COMPONENT NAME:**

Defense Information Systems Agency

**3. PIA APPROVAL DATE:**

05/03/22

### 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.**

C2 Software Factory (C2SF) provides software development, management, planning, and operations tools to Defense Information System Agency Program Offices (federal employees and federal contractors). This development and operations toolchain environment supports DISA SD PMO's mission objectives; providing them with the resources needed to complete these objectives efficiently and effectively. The C2 Software Factory operates in a closed environment and contains a suite of software applications to ingest code and automate the software build process for C2 software systems. In the future, the environment will also include test automation suites to vastly improve the speed and quality of test cycles of C2 system releases. The factory includes rich defect tracking and collaboration tools to augment the software build and test activities for the environment, facilitating the shared usage of software factory resources and the use of shared innovations and improvements across the C2 portfolio. The environment brings together the best of industry-standard DevSecOps tools and capabilities. Individuals requesting an C2SF account are required to provide an approved DD2875. The following PII is entered into the C2SF Database for user authentication purposes: Name(s), DoD ID Number, Work E-Mail Address, Organization, and Official Duty Telephone Phone.

**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)

Identification and Authentication (CAC/ECA Login)

**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 requiring access to C2SF will need to provide PII via the completion of a DD2875 for account creation purposes. An individual who objects to the collection of PII will not be able to secure an C2SF account.

**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.

By completing a DD Form 2875, individuals give consent to use of their PII for account creation and authentication.

**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

Authority - Executive Order 10450, and Public Law 99-474, the Computer Fraud and Abuse Act.

Principal Purpose - To record names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form.

Routine Uses - None

Disclosures - Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

**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)

Web/E-form collects basic CAC Number, First Name, Last Name, Role, and Organization

DD Form 2875 collects personal information, access justification and e-signature

**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    K890.14

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or <http://dpcltd.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 5.2 Item 20/DAA-GRS-2017-0003-0002
- (2) If pending, provide the date the SF-115 was submitted to NARA.
- (3) Retention Instructions.

Temporary. Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.

**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.

10 U.S.C. Chapter 8, Defense Agencies and Department of Defense Field Activities  
DoD Directive 5105.19, Defense Information Systems Agency (DISA)  
DoD Instruction (DoDI) 1000.25, DoD Personnel Identity Protection (PIP) Program  
DoDI 5200.46, DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC)  
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.

OMB Control Number: 0704-0415; Expiration Date: None