

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:

Electronic 2875 System (e2875)

2. DOD COMPONENT NAME:

United States Air Force

3. PIA APPROVAL DATE:

08/23/24

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 Electronic 2875 System (e2875) enables .mil users to submit System & Network Access requests electronically, with built in automatic routing and notification, providing electronic System Access Authorization Requests (SAAR). e2875 helps the warfighter quickly gain permission and access to IT systems, which require signed and documented DD2875 Forms. The following personal information about individuals is collected in the system: official duty address, work email address, official duty telephone, position/job title, rank/grade, DoD ID#, names, organization/office symbol/squadron/wing, and citizenship. It also includes investigation information, such as clearance level, and specifies if a user is Military, Civilian, or Contractor.

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)

To identify, verify, and validate the trustworthiness of individuals requesting access to DOD information systems. Individuals must be on a .mil network to access system.

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.

The submitting user can choose not to disclose the requested information. However, failure to do so will prevent further processing of their request.

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.

If the individual does not want to enter his/her information within the e2875 system, they can process the paper version of the DD Form 2875. The system states "Disclosure of this information is voluntary" with the Privacy Act Statement.

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, 9397; 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.

ROUTINE USES: NONE.

DISCLOSURE: DISCLOSURE OF THIS INFORMATION IS VOLUNTARY; HOWEVER, FAILURE TO PROVIDE THE REQUESTED INFORMATION MAY IMPEDE, DELAY OR PREVENT FURTHER PROCESSING OF THIS REQUEST. NOTE: RECORDS MAY BE MAINTAINED IN BOTH ELECTRONIC AND/OR PAPER FORM.

APPLICABLE SYSTEM OF RECORD NOTICE (SORN): F033 USSC A, INFORMATION TECHNOLOGY AND CONTROL RECORDS (March 03, 2008, 73 FR 11400).

DOD Directive 5200.28 authorizes collection of this information. The only use of this information is by the AIS Security Office and the System Management.

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.	United States Air Force (USAF) and United States Space Force (USSF) through access to e2875
<input checked="" type="checkbox"/> Other DoD Components (i.e. Army, Navy, Air Force)	Specify.	Defense Logistic Agency (DLA), DISA, Army, and Navy through access to e2875
<input type="checkbox"/> Other Federal Agencies (i.e. Veteran's Affairs, Energy, State)	Specify.	
<input type="checkbox"/> State and Local Agencies	Specify.	
<input type="checkbox"/> 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.	
<input type="checkbox"/> 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 checked="" type="checkbox"/> Individuals	<input type="checkbox"/> Databases
<input type="checkbox"/> Existing DoD Information Systems	<input type="checkbox"/> Commercial Systems
<input type="checkbox"/> Other Federal Information Systems	

Information is also pulled from DISA Global Content Delivery Service (GCDS).

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 type="checkbox"/> Information Sharing - System to System	<input checked="" type="checkbox"/> Website/E-Form
<input checked="" type="checkbox"/> Other (If Other, enter the information in the box below)	

Collected from the individual via website, existing DD2875 forms in e2875, and GCDS.

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://dpcl.d.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.

I. 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.

NI-AFU-90-03

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

(3) Retention Instructions.

T 33 – 25 R 01.00; Worldwide Military command & Control System, Threat Documentation, AIS Access Record @ AIS Activity/Facilities--
Destroy when superseded, obsolete or no longer needed

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.

EXECUTIVE ORDER 10450, 9397; AND PUBLIC LAW 99-474, THE COMPUTER FRAUD AND ABUSE ACT.

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 No. 0704-0630; OMB approval expires: 5/31/2025

NOTE: Sections 1 above is to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy. A Component may restrict the publication of Sections 1 if they contain information that would reveal sensitive information or raise security concerns.