

## 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:**

Judge Advocate Functional Server (JAFS)

**2. DOD COMPONENT NAME:**

United States Air Force

**3. PIA APPROVAL DATE:**

12/18/20

### SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

**a. The PII is:** (Check one. Note: foreign nationals are included in general public.)

- |  |  |
|--|--|
| <input type="checkbox"/> From members of the general public  | <input type="checkbox"/> From Federal employees and/or Federal contractors |
| <input checked="" type="checkbox"/> From both members of the general public and Federal employees and/or Federal contractors | <input type="checkbox"/> Not Collected (if checked proceed to Section 4)   |

**b. The PII is in a:** (Check one)

- |  |   |
|--|---|
| <input type="checkbox"/> New DoD Information System                    | <input type="checkbox"/> New Electronic Collection      |
| <input checked="" type="checkbox"/> Existing DoD Information System    | <input type="checkbox"/> Existing Electronic Collection |
| <input type="checkbox"/> 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.**

JAFS is a server and a hosting environment for all applications for the Air Force Judge Advocate General's Corps. The applications support programs that cover criminal law (military and civilian), claims administration, adverse actions, legal assistance, litigation management, recruiting, and personnel management. These are management areas where The Judge Advocate General is tasked through statute or regulation to provide support to the Air Force.

The types of personal information that may be collected includes an individual's name, address, e-mail address, phone number (home/cell), sex, age, social security number, marital status, citizenship, drivers license, official duty address, passport information, employment information, Air Force Personnel Center military records, education, place of birth, work email, DOB, race/ethnicity, education information, financial information, law enforcement information, off duty phone, position/title, rank/grade, personal email address, security information, child information, DoD ID, Legal status, other ID #, gender/gender information, photo, and records related to criminal acts by both military and civilian members.

**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 and stored in JAFS to verify the identify of Air Force personnel for personnel management, legal assistance, adverse actions, and those who submit claims against the Air Force. In addition, the information is used to manage criminal and civil litigation cases in federal courts. Individual provided information assists in verifying and paying claims, ensuring the right person is paid the right amount by the Defense Finance Accounting Service (DFAS). Furthermore, personnel records are used for data matching in Roster to assist The Judge Advocate General in his statutory duty to manage Air Force Judge Advocates.

All use of PII is mission related for the management of personnel, military justice matters, legal assistance, and claims against the government.

**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 may refuse to disclose any PII by not providing the information, but it would prevent verification that they are eligible to receive legal services.

**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.

Once PII is provided, it will be used to manage the case to completion.

**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

JAFs hosts applications, Privacy Act Statements are provided by these individual applications.

**h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? (Check all that apply)**

Within the DoD Component

Specify.

Information on individuals suspected of committing a criminal offense may be shared with DoD law enforcement agencies.

Other DoD Components

Specify.

Payment information from the hosted application is shared with DFAS to ensure payment of claims.

Other Federal Agencies

Specify.

Civil litigation case records may be shared with the Department of Justice for on going litigation case. Information may be released to congressional personnel if accompanied by a Privacy Act Release.

State and Local Agencies

Specify.

Contractor;s Name: Booze Allen

52.224-1 Privacy Act Notification.

As prescribed in 24.104, insert the following clause in solicitations and contracts, when the design, development, or operation of a system of records on individuals is required to accomplish an agency function:

Privacy Act Notification (Apr 1984)

The Contractor will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties.

(End of clause)

52.224-2 Privacy Act.

As prescribed in 24.104, insert the following clause in solicitations and contracts, when the design, development, or operation of a system of records on individuals is required to accomplish an agency function:

Privacy Act (Apr 1984)

(a) The Contractor agrees to—

(1) Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies—

(i) The systems of records; and

(ii) The design, development, or operation work that the contractor is to perform;

(2) Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a system of records on individuals that is subject to the Act; and

(3) Include this clause, including this paragraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a system of records.

(b) In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a system of records on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a system of records on individuals to accomplish an agency function, the Contractor is considered to be an employee of the agency.

(c)(1) "Operation of a system of records," as used in this clause, means performance of any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of rec

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.)



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 can come from an individual, existing DoD information systems (Air Force personnel records and Defense Finance and Accounting Service), and law enforcement records and agencies, including the Air Force Office of Special Investigations.

**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)  
 Face-to-Face 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

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.

Each system of records stored in application hosted by JAFS have a SORN. JAFS does not retrieve by name 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.

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

(3) Retention Instructions.

T&R: T 51 - 01 R 01.00, Personnel Data on Judge Advocates, Destroy 3 years after individual has separated or when no longer needed, whichever is sooner; T & RULE: T 51 - 01 R 02.00, Legal Opinions Establishing Precedent, Retire as permanent after reference requirements have been satisfied; T & R: T 51 - 01 R 03.00, Legal Opinions Information Copies, Destroy when no longer needed; T & R: T 51 - 01 R 10.00, Legal Assistance Administration, Destroy when no longer needed; T & R: T 51 - 01 R 14.00, Litigation, Destroy 25 years after end of year in which case is closed; T & R: T 51 - 01 R 35.00, U.S. Federal Magistrate Court, Destroy 3 years after case is closed; T & R: T 51 - 02 R 01.00, Patents, Copyrights and Trademarks (General Records) at AFLSA/JACP, Destroy after 25 years; T & R: T 51 - 02 R 03.00, Invention Disclosures at HQ USAF/JACP, Retire after 5 years and destroy 15 years thereafter; T & R: T 51 - 02 R 05.00, Patent Applications at AFLSA/JACP, Retire after 3 years, and destroy 17 years thereafter; T & R: T 51 - 02 R 09.00, Licenses, Releases and Assignments-Trademarks and Copyrights, Destroy 30 years after date of issue; T & R: T 51 - 02 R 11.00, Patent Infringement Claims, Preferred Licenses and Royalty Adjustments at AFLSA/JACP, Destroy 12 years after final settlement or judicial determination; T & R: T 51 - 04 R 01.00, General Administration HQ USAF Directives, Destroy when superseded or rescinded; T & R: T 51 - 04 R 03.00, Completed Claims Case Files, Destroy 1 year after the close of the fiscal year in which claims are settled; T & R: T 51 - 04 R 04.00, Completed Claims Case Files under Military and Civilian Employees Claim Act, Destroy 6 years after the close of the fiscal year in which claims are settled. Records frozen that relate to claims associated with Agent ORANGE or Vietnam-related claims (NAM). Retain indefinitely or until litigation is over; T & R: T 51 - 04 R 21.00, Tort Litigation Case Files at AFLOA, Destroy 5 years after FY in which the litigation is concluded; T & R: T 51 - 04 R 07.00, Claims Reports, Destroy 1 year after lapse of statute of limitations (Note: do not retire to records center); T & R: T 51 - 04 R 13.00, TITLE: Memorandum Opinions, Destroy after 6 months; T & R: T 51 - 05 R 02.00, TITLE: Notary Logs of Military Notaries, Destroy last duty station 2 years after the military notary completes service; T & R: T 51 - 05 R 05.00, DD Form 2793, Volunteer Agreement for Appropriated Activities or Nonappropriated Fund Instrumentalities, Destroy 3 years after the volunteer relationship has terminated; T & R: T 51 - 05 R 06.00, DD Form 1175, Legal Assistance Record, Destroy when information is entered in WebLIONS

Note: Among the disposition(s) cited in this field, the one with the longest retention time will be used on the system's records data.

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.