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:

Aircraft and Personnel Automated Clearance System (APACS)

2. DOD COMPONENT NAME:

United States Air Force

3. PIA APPROVAL DATE:

05/03/21

SecAF is designated the DoD Executive Agent for the DoD Foreign Clearance Program per DoDD 4500.54E and OPR to manage APACS

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

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

- [ ] From members of the general public
- [ ] From Federal employees and/or Federal contractors
- [x] From both members of the general public and Federal employees and/or Federal contractors
- [ ] Not Collected *(if checked proceed to Section 4)*

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

- [ ] New DoD Information System
- [ ] New Electronic Collection
- [x] 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.

APACS is a web-based application, currently hosted on the DISA milCloud service, is operated by the U.S. Air Force due to the Secretary of the Air Force being designated as the Department of Defense (DoD) Executive Agent for the DoD Foreign Clearance Program.

It is designed to aid DoD mission planners, aircraft operators and DoD personnel in meeting host nation aircraft diplomatic and personnel travel clearance requirements outlined in the DoD Foreign Clearance Guide. APACS provides requesting, approving, and monitoring organizations (i.e., country clearance approvers at U.S. Embassies, Geographical Combatant Commands (GCC) theater clearance approvers, and Office of the Secretary of Defense (OSD) special area clearance approvers) access to a common, centralized, and secure database that contains all the information required to process/approve foreign travel clearances.

Types of PII Collection: Name(s); Position/Title; Rank/Grade; Employment Information; Security Information; DoD ID Number; Citizenship; Work E-mail Address; Official Duty Address; Official Duty Telephone Phone; Personal E-mail Address; Home/Cell Phone; Passport Information; Place of Birth; Birth Date; Emergency Contact.

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 used by in-country U.S. Embassy approvers to grant country travel clearances, Geographical Combatant Commands approvers to grant theater travel clearances and by the Office of Secretary of Defense for Policy approvers to grant special area travel clearances. Aircrew PII information for verification, identification and authentication of travelers for aircraft and personnel travel clearances.

e. Do individuals have the opportunity to object to the collection of their PII? [x] 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.

User disclosure of PII is voluntary. However, failure to furnish the requested information may result in denial of aircraft and/or personnel travel clearance requests by country / theater / special area clearance approvers respectively.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [x] 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.

Level of required PII is specific to the traveler's destination and type of the required travel clearance (i.e., official, leave). If the individual withhold their consent, it may result in denial of aircraft and/or personnel travel clearance.

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: 10 U.S.C. 7013, Secretary of the Army; 10 U.S.C. 8013, Secretary of the Navy; 10 U.S.C. 9013, Secretary of the Air Force; 22 U.S.C. 4801, Findings and purpose; 22 U.S.C. 4802, Responsibility of Secretary of State; and 22 U.S.C. 4805, Cooperation of other Federal Agencies; Public Law 99-399, Omnibus Diplomatic Security and Antiterrorism Act of 1986; Department of Defense Directive 4500.54E, DoD Foreign Clearance Program; DoD Directive 5400.11, Privacy Program; NIST.SP.800-53r4, Security and Privacy Controls for Federal Information Systems and Organizations; Privacy Act of 1974.

Purpose: This system is a web-based application operated by the U.S. Air Force due to the Secretary of the Air Force being designated as the Department of Defense (DoD) Executive Agent for the DoD Foreign Clearance Program. It is designed to aid DoD mission planners, aircraft operators and DoD personnel in meeting host nation aircraft diplomatic and personnel travel clearance requirements outlined in the DoD Foreign Clearance Guide. APACS provides requesting, approving, and monitoring organizations (i.e., country clearance approvers at U.S. Embassies, Geographical Combatant Commands (GCC) theater clearance approvers, and Office of the Secretary of Defense (OSD) special area clearance approvers) access to a common, centralized, and secure database that contains all the information required to process/ approve foreign travel clearances.

Routine Use:
a. To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature.

b. To any component of the Department of Justice for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent.
c. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the DoD or other Agency representing the DoD determines that the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.
d. To the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 U.S.C. §§ 2904 and 2906.
e. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.
f. To appropriate agencies, entities, and persons when (1) the DoD suspects or has confirmed that there has been a breach of the system of records; (2) the DoD has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.
g. To another Federal agency or Federal entity, when the DoD determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.
h. To contractors, grantees, experts, consultants, students, and others performing or working on a contract , service, grant, cooperative agreement, or other assignment for the federal government when necessary to accomplish an agency function related to this system of records.
i. To appropriate Federal, state, local, territorial, tribal, foreign, or international agencies for the purpose of counterintelligence activities. This routine use complies with U.S. law or Executive Order, or for the purpose of executing or enforcing laws designed to protect the national security or homeland security of the United States, including those relating to the sharing of records or information concerning terrorism, homeland security, or law enforcement.
j. To a domestic or foreign entity entering into a public-private partnership with the Defense POW/MIA Accounting Agency (DPAA). This routine use complies with 10 U.S.C. 1501a, when DPAA determines such disclosure is necessary to the performance of services DPAA agrees shall be performed by the partner.

Disclosure: User disclosure of PII is voluntary. However, failure to furnish the requested information may result in denial of aircraft and/or personnel travel clearance requests.

System of Records Notice: F011 AF A3 B DoD - DoD Foreign Clearance Program Records (January 03, 2012, 77 FR 94).

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.	To appropriate agencies, entities, and persons when (1) The Department of Defense (DoD) suspects or has confirmed that the security or confidentiality of the information in the system of records; (2) the DoD has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.
☒ Other DoD Components	Specify.	In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the DoD or other Agency representing the DoD determines that the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.
☒ Other Federal Agencies	Specify.	To any component of the Department of Justice for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent. To the National Archives and Records Administration for the purpose of records management inspections conducted. This routine use complies with 44 U.S.C. §§ 2904 and 2906. To another Federal agency or Federal entity, when the Department of Defense (DoD) determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach. To a domestic or foreign entity that has entered into a public-private partnership with the Defense POW/MIA Accounting Agency (DPAA). This routine use complies with 10 U.S.C. 1501a, when DPAA determines that such disclosure is necessary to the performance of services DPAA has agreed shall be performed by the partner.

☒	State and Local Agencies	Specify.	To appropriate Federal, State, local, territorial, tribal, foreign, or international agencies for the purpose of counterintelligence activities. This routine use complies with U.S. law or Executive Order, or for the purpose of executing or enforcing laws designed to protect the national security or homeland security of the United States, including those relating to the sharing of records or information concerning terrorism, homeland security, or law enforcement. To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature
☒	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.	Contractor Name: Science Applications International Corporation (SAIC) FAR 52.224-1 – Privacy Act Notification, 52.224-2 – Privacy Act, and FAR 39.105 clauses are not included in the contract. However, the contract contains a clause on paragraph 4.5.3 as: "Non-Disclosure Agreement (NDA) – Contractor personnel shall not divulge or release data or information developed or obtained in the performance of this requirement, until made public or specifically authorized by the Government. The Contractor shall not use, disclose, or reproduce third party companies' proprietary data, other that as authorized and required in performance of this requirement. Personnel working on this project will be required to sign a Non-Disclosure Agreement (NDA) immediately upon their start on the requirement. The Contractor's procedures for protecting against unauthorized disclosure of information shall not require DoD employees or members of Armed Forces to relinquish control of their work product, whether classified or not, to the Contractor." FAR 52.224-1 – Privacy Act Notification, 52.224-2 – Privacy Act, and FAR 39.105 clauses will be included in the next PWS scheduled to be renewed on/about May 2021.
☒	Other *(e.g., commercial providers, colleges)*.	Specify.	To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government when necessary to accomplish an agency function related to this system of records.

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

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.