


TAB 1 – APACS milCloud home page

UNCLASSIFIED

APACS



AIRCRAFT AND PERSONNEL AUTOMATED CLEARANCE SYSTEM

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

At any time, the USG may inspect and seize data stored on this IS.

- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests – not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

I agree to the terms of the [User Agreement](#)

Tab 2 – APACS milCloud User Agreement

APACS

AIRCRAFT AND PERSONNEL AUTOMATED CLEARANCE SYSTEM



Aircraft and Personnel Automated Clearance System (APACS) User Agreement

STANDARD MANDATORY NOTICE AND CONSENT PROVISION

By acknowledging this document, you consent that when you access Department of Defense (DoD) information systems:

- You are authorizing APACS to collect, use, maintain, and share personally identifiable information (PII) with the appropriate travel clearance organizations. [See privacy act statement.](#)
- You are authorizing APACS to reuse any previously collected PII as necessary.
- You are authorizing APACS to use all PII that was not initially described in the privacy act statement.
- You are accessing a U.S. Government (USG) Information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government-authorized use only.
- You consent to the following conditions:
 - The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
 - At any time, the U.S. Government may inspect and seize data stored on this information system.
 - Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.
 - This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy.
 - Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:
 - Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.
 - The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.
 - Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.
 - Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.
 - A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.
 - These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.
 - In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (i.e., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.
 - All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

Privacy Act Statement

Authority: 10 U.S.C. 3013, Secretary of the Army; 10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 8013, 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: Congressional Inquiries Disclosure Routine Use: Disclosure from a system of records maintained by a DoD Component may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

Disclosure of Information to the General Services Administration Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to the General Services Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

Disclosure of Information to the National Archives and Records Administration Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

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).

User Consent to Collection and Disclosure of Personally Identifiable Information (PII)

APACS collects Personally Identifiable Information (PII). By using this system, the user consents to the collection, use, maintenance, dissemination and retention of PII. All PII collected, used, maintained, disseminated and retained by APACS is used only for the identification of user accounts, for the processing of aircraft and personnel travel requests and for generating reports to approver organizations. PII may be viewed by all roles involved in the stated purposes above, including system administrators and software developers within the capacity of troubleshooting and issue resolution. All PII is safeguarded in a manner consistent with the NIST.SP.800-53r4 and DoD Directive 5400.11, Privacy Program. Public disclosure of PII is in accordance with the Privacy Act of 1974.

APACS

AIRCRAFT AND PERSONNEL AUTOMATED CLEARANCE SYSTEM



Do not use bookmarks/bookmarked URL webpages to access APACS.
Use the most recent version of APACS by clearing the internet browser history/cache then type in:
<https://apacs.dtic.mil/apacs/>
Please contact local IT Department if assistance is needed clearing browser history/cache.

APACS does not send unsolicited e-mails to users. If you receive unsolicited e-mails, do not "click" on any provided URL link(s). If you elect to go to the site, type the URL into your browser instead. Hovering your pointer over the URL before clicking will allow you to see the actual URL destination. In light of ongoing DoD cyber security concerns, users should be aware of potential e-mail spoofing fraud attempts seeking unauthorized access to protected data or providing malicious credential harvesting URL links in an effort to obtain credentials. If the e-mail does not appear legitimate, delete it. If you have any questions or concerns, please contact your appropriate IA personnel.

[View Privacy Act Statement](#)

Welcome to the Aircraft and Personnel Automated Clearance System (APACS)

Use APACS to create, review and submit your Aircraft and Personnel travel requests

Sign in to APACS

Username:
Password:

[Need Login Assistance?](#)

CAC Sign in to APACS

[Need CAC Login Assistance?](#)

New Accounts & Help

- [Sign up to use APACS](#)
- [Help](#)
- [FAQ](#)

Tab 5 - APACS milCloud Internal Home (after login)

https://apacs.milcloud.mil/apacs/apacsservlet?cmd=apacsLogin

APACS

View Favorites Tools Help

ZIKS VIFUS
Refer to the following websites for the latest list of countries where the Zika virus is present:
http://travel.state.gov/content/passports/en/go/Zika.html
http://www.cdc.gov/zika/index.html

Aircraft Requester | Personnel Requester | FCG Rules | My Account | Admin | Message Center

Get Help Using APACS:
[Aircraft Requester Help](#), [Personnel Requester Help](#), [Help](#)

Release Update:
The latest release of APACS includes the following enhancements:

- Overall application enhancement to achieve compliance with DISA Security Technical Implementation Guides (STIG)
- Overall application enhancement to achieve compliance with DISA Burp Scan Web Vulnerability Report
- Preventing cross-site request forgery (CSRF)
- Addressed path-relative stylesheet (CSS) imports

To view previous and latest list of fixes, enhancements and new features of APACS click on [Release 59.1 \(06/08/2017\)](#)

Accessibility/Section 508:
The U.S. Department of Defense is committed to making its electronic and information technologies accessible to individuals with disabilities in accordance with Section 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended in 1998 < Caution-http://www.access-board.gov/the-board/laws/rehabilitation-act-of-1973#508 > . Send feedback or concerns related to the accessibility of this website to: DoDSection508@osd.mil < Caution-mailto:DoDSection508@osd.mil > . For more information about Section 508, please visit the DoD Section 508 website < Caution-http://dodcio.defense.gov/DoDSection508.aspx > . Last Updated: 08/06/2013

System of Records Notice (SORN):
To view the DoD Foreign Clearance Program - System of Records Notice (SORN) click [here](#).

Office of Management and Budget (OMB):
OMB 0701-XXXX (Pending)

Tab 6 – APACS milCloud Traveler Notes (PII Requirements – Netherlands)

Add Traveler

Traveler Assignments: Country Netherlands Arrival 15:16:20L Nov 2017 Departure 17:16:20L Nov 2017

Name (Last, First MI):

Service:

Rank/Rating:

Country of Citizenship:

Security Clearance:

ICASS:

AT Level 1 Training:

SERE Training:

Category:

Grade:

Highest Ranked:

Job Title:

Organization:

Mission Training Requirements:

ISOPREP:

Netherlands
(1) Passport number or the DoD ID number.
(2) Date of birth.
(3) Cell phone number of Advance/Lead agent.
(4) Fax number for unit being visited.

Traveler Notes:

Add Traveler Cancel

Tab 7 – APACS milCloud Security Clearance Requirement (Netherlands)

Add Traveler

Traveler Assignments:	Country	Arrival	Departure
	<input checked="" type="checkbox"/> Netherlands	15:16:20L Nov 2017	17:16:20L Nov 2017

Name (Last, First MI):	<input type="text"/>	Category:	<input type="text" value="DOD-MILITARY"/>
Service:	<input type="text" value="-- Choose One --"/>	Grader:	<input type="text" value="-- Choose One --"/>
Rank/Rating:	<input type="text"/>	Highest Ranked:	<input type="checkbox"/>
Country of Citizenship:	<input type="text"/>	Job Title:	<input type="text"/>
Security Clearance:	<input type="text" value=" "/>	<small>Information entered in this field does not validate the security clearance nor does it authorize access to classified information or secure facilities. If required for this visit, security clearance information must be passed via Joint Personnel Adjudication System (JPAS) or other appropriate method. Travelers with Sensitive Compartmented Information (SCI) access shall report anticipated foreign travel (AW) with DoDM 5105.21, Vol 3.</small>	
ICASS:	<input type="text"/>	ISOPREP:	<input type="text"/>
AT Level 1 Training:	<input type="text" value=""/>	Traveller Notes:	<input type="text" value=""/>
(yyyy-MM-dd)			
SERE Training:	<input type="text" value=""/>		
(yyyy-MM-dd)			