

DEPARTMENT OF HOMELAND SECURITY

U.S. Coast Guard

TPAX/WINIATS USER ACCESS AUTHORIZATION & APPROVING OFFICIAL (AO) DESIGNATION

Please fill out online or print neatly! This authorization supersedes previous applications

1. User's Name (Last, First, MI.) (Please print)	2. Rank/Rate:	3. Employee ID (SSN for non-employees)
--	---------------	--

4. Official Duty Station & OPFAC	5. Area Code & Work Phone Number:	6. e-Mail address:
----------------------------------	-----------------------------------	--------------------

7. User Role Description (see instructions)(Include current roles, this authorization supersedes all of your previous authorizations):

TPAX (Travel Preparation & Examination System Permissions)

TPAX AO (Authorizing Official) Permissions **Travel Manager - Primary/Alternate**

Date of Expiration:
(Will automatically expire one year from date of command signature)

Advance Signature Proxy Permissions

Date of Expiration:
(Will automatically expire one year from date of command signature)

Create "Non-CG Employee" Self Service User Profile

Note: Contractors are not allowed to complete travel claims nor do they have access to TPAX.
****Non-CG Employees Must fill out blocks 1-6, 8-12 and provide SSN in 3.**

Blocks 8 to 12 required only for **Non-CG Employee** requests

8. Home Address: Street Address, Apt #:

9. Home Address: City, State, Zip Code:

10. Check all that apply as well as status within branch:

CGES	USMC	Civilian DOD Employee
USCG AUX	USAF	Chaplain
USPHS	USN	Active Duty
USA		Reserve Duty

Other: (specify)

11. USCG Work Address: Street Address

12. USCG Work Address: City, State, Zip Code

Winlats Access Permissions (PPC TVL Only)

Examiner Permissions
 Auditor Permissions
 Distribution Permissions
 System Administrative Restricted Permissions
 System Admin Permissions (full)
 Super User Permissions (system suppt users only)

Web/Image Now Access Permissions (PPC TVL Only)

Examiner Permissions (all travel folders)
 Exception:
 System Admin Permissions (all travel folders)

Revocation:

With the exception of non-employees, TPAX/WINIATS roles are automatically terminated upon PCS, separation, retirement, reassignment of duties (Fleet-Ups) and change of organization (inter-office transfer). AO, Advance Signature Proxy and Customer Service Representative Permissions automatically expire one year from the date of the command signature. Submit a new application, annually, to retain these permissions.

Users who have been reassigned (PCS, Change of Department IDs) will retain Self-Service access.

The user role termination process is kicked off by submission of a PCS departing endorsement. If the member submits a new access form, and it is processed by PPC before the SPO submits the PCS departing endorsement, the system will terminate the new access. Please be sure to submit transactions in a timely manner.

If Revocation is for a non-employee or is due to reasons other than those listed above contact PPC Customer Care via on-line trouble-ticket at <http://www.uscg.mil/ppc/ccb> or <http://cgweb.ppc.uscg.mil/ccb/> or via email at PPC-DG-CustomerCare@uscg.mil

Customer Service Representative Permissions (PPC Only)

Date of Expiration:
(Will automatically expire one year from date of command signature)

System Administrator (PPC TVL Only)

Date of Expiration:

13. **CMD Designation (Signature & printed name, Rank, Title (CO/OIC, XO/XPO or HQ/PSC/PPC/FORCECOM/DCMS/DIST/ or Sector Branch Chief):**

I certify that the access I have authorized is based on an official need. I'm aware of the general functionality I have authorized and I'm aware of what this will allow this member to complete. This member has demonstrated that they are knowledgeable in the use of the program I've authorized and has my confidence that they will diligently make entries and if in doubt they will seek assistance. I also acknowledge that if I lose confidence in this member for any reason I have a responsibility to withdraw this authorization.

Signature AND PRINTED or TYPED Name,	Rank,	Title,	Phone	OPFAC	Date:
---	-------	--------	-------	-------	-------

For User Reference

Your TPAX Profile should be updated within 05 business days from the date this form is received at PPC Travel.

TPAX Profiles must be set up with user's password and general information required prior to submitting request for permissions other than self service. Designation requests without basic profile information already entered by traveler will not be updated by PPC.

Acknowledgment: I understand that I am authorized to access the TPAX/WINIATS system and that accessing it for purposes beyond the Scope of Authorization is a violation of Federal law (18 U.S.C. 1030 et al) (Note: Refer to the Automated Information Systems (AIS) User Acknowledgement Form (CG-5500A), which is required for all U.S. Coast Guard AIS users, it contains the full Scope of Authorization and Acknowledgement.). **By signing the User Signature below, I certify that I have read and understand the Statements of Responsibility and Liability, located on page 2 of this document, for each of the permissions assigned above.**

Privacy Act Statement

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 identifying individuals requesting access to U. S. Coast Guard (USCG) systems and information. NOTE: Records may be maintained in both electronic and/or paper form.

ROUTINE USES: None.

DISCLOSURE: Disclosure of this information (including your SSN if not a member/employee of the USCG) is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

14. User's Signature:	Date:
-----------------------	-------

(For PPC Use Only) TPAX/Winlats Access Systems Administrator & CS		Fax to: (785) 339-2296	
Operator ID (if not = to Emplid):	OPRCLASS:	TPAX/Winlats System Administrator Signature:	Date:

CG-7421/2 (Rev. 06-11) Instructions

- Fax the completed form to PPC at the number on the form ((785) 339-2296)
- Retain the original form in the unit's files until the member departs the unit.
- TPAX/Winlats termination should be part of your unit checkout process.

All TPAX/Winlats System permissions:

Read and be familiar with:

- Authorizing Official Online Training Course (<http://www.uscg.mil/ppc/travel/aocert/1-Overview/>)
- Contractor's TPAX User Guide at PPC Website (<http://www.uscg.mil/ppc/webtpax/index.htm>)
- JFTR, Temporary Duty (TDY) Travel Entitlements (<http://www.defensetravel.dod.mil/site/travelreg.cfm>)
- CG Supplement to JFTR, (http://www.uscg.mil/directives/cim/4000-4999/CIM_4600_17.pdf)
- Chapter 2, 3PM. (<http://www.uscg.mil/PPC/3pm.asp>)
- Federal Travel Regulations (FTR) (<http://www.gsa.gov/federaltravelregulation>)
- The Coast Guard Freedom of Information (FOIA) And Privacy Acts Manual (http://www.uscg.mil/directives/cim/5000-5999/CIM_5260_3.pdf)

TPAX Authorizing Official Statement of Responsibility and Liability:

TPAX AO Statement of Responsibility & Liability: AOs have the authority to review & approve travel payment transactions in TPAX and therefore, shall become knowledgeable in the matters of document(s) being approved. TPAX AO's have broad authority to determine when TDY travel is necessary to accomplish the unit's mission, authorize travel, obligate unit travel funds, approve trip arrangements & authorize travel expenses incurred in connection with the travel. TPAX AOs shall ensure documents are carefully reviewed before approval and not signed only as a matter of formality. The TPAX AO shall not compromise system integrity by revealing their personal passwords. The TPAX AO is fully accountable to the Coast Guard and may be found liable for erroneous or improper payments. TPAX AO designation is terminated with a permanent transfer, inter-unit transfer, or when deemed necessary by competent authority.

All AO permissions will automatically expire one year (1 year) from the date of command signature, when member changes OPFACs, separates from the CG or changes status (*i.e. from active to reserve components*).

TPAX Advance Signature Proxy Statement of Responsibility and Liability (SPO Designation):

TPAX AdvSigProxy Statement of Responsibility & Liability: AdvSigProxy have the authority to prepare Travel Advances on the member's behalf in TPAX, electronically sign for the member and forward to the appropriate AO and therefore, shall become knowledgeable in the matters of document(s) being created. TPAX AdvSigProxies have broad authority to process advances in connection with the travel on behalf of any member within their area of responsibility (*typically any unit that fall under the SPO*). TPAX AdvSigProxy shall ensure documents are carefully reviewed before forwarding to AO. The TPAX AdvSigProxy shall not compromise system integrity by revealing their personal passwords or personal information contained within the TPAX system. The TPAX AdvSigProxy is fully accountable to the Coast Guard and may be found liable for erroneous or improper payments and may be held accountable for failure to follow the Privacy Act. TPAX AdvSigProxy designation is terminated with a permanent transfer, inter-unit transfer, or when deemed necessary by competent authority. By my signature above I certify I understand and agree to this Statement of Responsibility and Liability.

All AdvSigProxy permissions will automatically expire one year (1 year) from the date of command signature or when member changes OPFACs or separates from the CG or changes status (*i.e. from active to reserve components*).

TPAX Customer Service Representative Statement of Responsibility and Liability:

TPAX CSR Statement of Responsibility & Liability: CSR have the authority to review all CG travel accounts in TPAX, to assist members with questions, reset of passwords, and necessary instruction and

therefore, shall become knowledgeable in the matters of travel regulations for both military and civilian personnel, privacy act regulations, and the operation of TPAX. TPAX CSR shall not compromise system integrity by revealing their personal passwords or personal information contained within the TPAX system. The TPAX CSR is fully accountable to the Coast Guard and may be held accountable for failure to follow the Privacy Act. TPAX CSR designation is terminated with a permanent transfer, inter-unit transfer, or when deemed necessary by competent authority.

All Customer Service permissions will automatically expire one year (1 year) from the date of command signature or when member changes OPFACs or separates from the CG or changes status (*i.e. from active to reserve components*).

TPAX System Administrator Statement of Responsibility and Liability:

TPAX SA Statement of Responsibility & Liability: TPAX SA have the broad authority within TPAX.....The TPAX SA is fully accountable to the Coast Guard and may be found liable for erroneous or improper payments and may be held accountable for failure to follow the Privacy Act. TPAX SA designation is terminated with a permanent transfer, inter-unit transfer, or when deemed necessary by competent authority.

Winlats Examiner Statement of Responsibility and Liability:

An Examiner is the individual primarily responsible for the overall processing of travel payments

Winlats Auditor Statement of Responsibility and Liability:

An Auditor is the individual responsible for reviewing travel claims that have been processed and are flagged for audit. When a claim has been flagged by IATS for audit, an individual with Auditor Function capabilities must access the flagged block and either review the flagged claim on-screen, or review a printed audit report. The Auditor must review every input screen for a claim flagged for audit.

Winlats Disbursing Statement of Responsibility and Liability:

An individual with Disbursing capabilities is responsible for preparing a block of processed claims for payment. In addition, this individual must release the processed blocks and carries the same accountability as a PAO.

Winlats System Administrator (limited/full) Statement of Responsibility and Liability:

The System Administrator is the individual responsible for the overall operation of IATS and controlling the work flow throughout the system. System Administrators are responsible for the set-up and configuration of IATS for the particular travel office. In addition, System Administrators perform the following additional functions: Performing system maintenance; Establishing user accounts; Assigning/re-assigning blocks and claims; Deleting completed blocks; Deleting un-needed traveler or travel order details; Debt management; Importing and updating system rates files; Processing interfaces between accounting, disbursing, and personnel systems; Generating management reports; Running utility programs.

Winlats SuperUser Statement of Responsibility and Liability:

When user accounts are created by the System Administrator, a View mode must be established. The functions a user may perform are dependent upon the View mode associated with their user ID. The Super User View allows the user to switch between various View modes without logging out and logging back in with a different user ID. When the Super User logs-in initially, their View mode defaults to System Administrator.