

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

<b>Department of Homeland Security</b> U. S. Coast Guard CG PPC 7421/2 (Rev. 02/2009)		<b>Direct-Access User Access Authorization and Payment Approving Official (PAO) Designation</b>	
1. User's Name (Last, First, MI.) (Please print or type)		2. Rank/Rate:	3. Employee ID # (Not SSN)
4. Dept ID & Unit Name (Include Staff Symbol)	5. Area Code & Phone Number:		6. e-Mail address:
7. User Role Description (see instructions)(Include current roles, this authorization supersedes all of your previous authorizations): <input type="checkbox"/> <b>CGSSCMD</b> --Command User (evals, drills, Airport Terminal, etc.) <input type="checkbox"/> <b>CGEMPREV</b> -- Employee Review Only (not needed if you have CGSSCMD or CGHRS) <input type="checkbox"/> <b>CGRSVDRL</b> – Schedule, Edit and Approve Reserve IDT Drills (Only) <input type="checkbox"/> <b>CGRSVMGR</b> – Create, review, and endorse requests for reserve orders. <input type="checkbox"/> <b>CGAIRTRM</b> --Airport Terminal Only (Relocation Specialists/Housing Office) <input type="checkbox"/> <b>CGFIELDADM</b> --Unit with access to Member Competencies (Quals, Awards & Schools) (Route request through your Servicing Personnel Office – Per PPCINST M1000.2a, Chap 1.) <input type="checkbox"/> <b>CGGWIS</b> --Global Workforce Inquiry System (Provides View Only Access to Personal Data) <input type="checkbox"/> <b>CGHRS</b> -- (SPO) DEPT ID _____ <input type="checkbox"/> <b>CGAPPL</b> – Applicant Data (Use with CGHRS for accessions. This role is necessary to create applicant IDs. <b>Cannot be selected with CGHRSUP.</b> ) <input type="checkbox"/> <b>CGHRSUP</b> —(SUPERVISOR, Payment Approving Official (PAO)) (Application must be approved by PPC (MAS)). ACO/MAS: Name/Sign: _____ <input type="checkbox"/> <b>CGMRS</b> — Medical Readiness System Clinical Access (Med care providers) <input type="checkbox"/> <b>CGTRNOFF</b> – Electronic Training Request (ETR). Unit ESOs. <input type="checkbox"/> <b>CGFTESO</b> – Unit Educational Services Officer. Unit ESOs. <input type="checkbox"/> <b>CGSECURN</b> --Unit Security Manager (View Only) <input type="checkbox"/> <b>CGSECUVW</b> --Area/Dist Security Manager (View Only). Fax completed form to COMDT (CG-86) at <b>202-372-3950</b> for approval. CG-86 will forward to PPC. CG-86 Name/Sign: _____ -----HQ/CGPC/TQC/TRACENs/ISC(pf/fot)/PPC <u>Only</u> ----- <input type="checkbox"/> <b>CGTRNFAC</b> --Training Center (TAS Course Sessions) <input type="checkbox"/> <b>CGTRNTQC</b> --TQC/TAS Course Scheduler <input type="checkbox"/> <b>CGASGN</b> --CGPC (epm/opm) or ISC(fot) Assignment Officer <input type="checkbox"/> <b>CGRSVISC/CGRSVORD</b> —Reserve Orders Approval/Funding, ISC(fot) only. <input type="checkbox"/> Others Not Listed. Please describe what you need to access in Direct-Access.		<b>Scope of Authorization</b> Subject to the limitations that follow, the user is authorized access to the computer systems identified above. This authorization contains no implied authorization to access any computer system of the United States Government not specifically identified herein. Authorization will be revoked upon separation, retirement, reassignment of duties, change of organization or when determined by the Information Systems Security Officer to be in the best interest of the Government. <b>WARNING: Only Authorized Users May Use These Systems.</b> To protect these systems from unauthorized use and to ensure that these systems are functioning properly, system administrators monitor these systems. Individuals using these systems without authority, or in excess of their authority, are subject to having all of their activities on these systems monitored and recorded by system personnel. In the course of monitoring individuals improperly using these systems, or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using these systems expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, management may authorize system personnel to provide the evidence of such monitoring to law enforcement officials.	
<b>8. Authorizing Official (Signature &amp; Typed or printed name, Rank, Title (CO/OIC, XO/XPO or HQ/PSC/AREA/MLC/DIST Branch Chief) &amp; Phone</b> 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 <b>AND PRINTED or TYPED</b> Name, Rank, Title (see instructions), Phone			9 Date:
<b>Acknowledgment:</b> I understand that I am authorized to access the Direct-Access 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). My password meets the DOT Information Systems Security requirements, and I may be held responsible for my inappropriate protection or sharing of my password. I understand that prior to entering any transactions into Direct-Access I must be knowledgeable on the validity of the entry, the impact of that entry within Direct-Access, and the impact on the member. I also understand that I must cite appropriate source documents (e.g. award citations, letters of authorization, etc.) prior to entering data into Direct-Access. I understand that I am fully accountable to the Coast Guard and may be found liable for erroneous or improper entries/payments until properly relieved of accountability. Personal monetary liability, adverse personal evaluation, and or further administrative or disciplinary actions may result if I am found negligent in the performance of my duties.			
10. User's Signature:			11. Date:
(For PPC Use Only) Direct-Access Security Administrator and PAO Validation/Designation			<b>Fax to: (785) 339-2297</b>
Operator ID (if not = to Emplid):	OPRCLASS:	Direct-Access Security Administrator Signature:	Date:

Previous editions are obsolete and may not be used.

**Revocation of Access Authority**

Complete this section when the access needs to be terminated for any reason other than transfer or termination. Fax it to (785) 339-2297.

12. User's Name (Last, First, MI.) <b>(Please print)</b>	13. Rank/Rate:	14. Employee ID # <b>(Not SSN)</b>
<p><b>15. Notice to User:</b> You are hereby notified that the above access authorization has been revoked. The associated login name and password are still valid for access to self-service items. To access a United States Government computer without authorization is a violation of Federal law (18 U.S.C. 1030 et al). <i>Authorization to access another United States Government computer system does not imply reinstatement of the authorization being revoked.</i></p> <p>Unit Attached to: _____</p> <p><b>Acknowledgment</b> (user's signature): _____ <b>(Date):</b> _____</p>		
<p><b>16. Authorizing Official</b> (<i>Signature AND Typed or printed name, Rank, Title and Phone Number</i>):</p> <p>_____</p> <p>Name, Rank, Title (e. g. CO/OIC, XO/XPO, By direction), Phone Number</p>		17. Date:
18. <i>Direct-Access Security Administrator</i> Signature:		19. Date:

**Instructions**

- Fax the completed first page of the form to the PPC Customer Care Center at the number on the form.
- Retain the original form in the unit's files until the member departs the unit.
- If access needs to be terminated, prior to member's PCS departure or separation, have the user sign and date the *Revocation of Access Notice* section of the form. Fax the complete form (both pages) to PPC at (785) 339-2297 (Place page 2 of the form before page 1 so we know it's a termination).
- Please see Chapter 1 of the Personnel and Pay Procedures Manual, PPCINST M1000.2 (series) for complete instructions (<http://www.uscg.mil/hr/psc/pppm/chap01.pdf>).

**Automatic Termination of DA User Access Upon Separation or PCS/Fleet Up**

Do not complete *Revocation of Access Authority* section of the form for members who transfer or separate. The Direct Access Roles are automatically terminated upon PCS, separation, retirement, reassignment of duties (Fleet-Ups) and change of organization (inter-office transfer).

Note: 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.