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

**U.S. DEPARTMENT OF HOMELAND SECURITY**
U. S. Coast Guard
CG-7421F (Rev. 05-10)

# Direct Access II (Global Payroll) User Access Authorization/Revocation

| | | |
|---|---|---|
| 1. User's Name (Last, First, MI.) (Please print) | 2. Rank/Rate/Grade: | 3. Employee ID # |
| 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 supercedes all of your previous authorizations):

- □ **CG_GP_VA_ACCESS** – DVA Queries
- □ **CG_RAS_TECHNICIAN**—Update Payee
- □ **CG_RAS_SUPER_TECH** – Full Access Payee
- □ **CG_RAS_AUDITOR** – Auditor Functions
- □ **CG_RAS_DECEDENT_PROC** – Processing of RAS Decedents
- □ **CG_RAS_PAY_MANAGER** – Pay Management
- □ **CG_RAS_TAX_PROC** – Tax Schedules and Internal Audit
- □ **CG_VIEWGP_HR** – View Payee
- □ **CG_RUN_REPORTS** – Reports
- □ **CG_RAS_PAY_FINALIZE** - Ability to finalize a payroll
- □ **CG_FINCEN_USER** - View access to reconciliation pages
- □ **CG_SYSTEM_ADMIN** - Run interfaces, view system functions (workflow, integration, process)
- □ **CGDEVELOPER** - Access to migrate objects (IBM role)
- □ **CGDEVELOPER_VIEWONLY** - Access to view objects (architect role)

## Scope of Authorization

*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.

**WARNING: Only Authorized Users May Use These Systems.**

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.

8. **Authorizing Official** *(Signature, **Typed or printed** name, Rank, Title (*CO/OIC, XO/XPO or HQ/PPC/AREA/DIST Branch Chief) *& Phone Number):*
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, **PRINTED or TYPED** Name, Rank, Title (see instructions), Phone | 9 Date: |

**Acknowledgment**: 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.

**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 is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

| | |
|---|---|
| 10. User's Signature: | 11. Date: |

| | | | |
|---|---|---|---|
| ***(For PPC Use Only) Direct-Access Security Administrator And PAO Validation/Designation*** | | **Fax to: (785) 339-2297** | |
| Operator ID (if not = to Emplid): | OPRCLASS: | ***Direct-Access Security Administrator* Signature**: | Date: |

## *Revocation of Access Authority*

Complete this section when the user is reassigned, separates from the service/terminates employment or the access needs to be terminated for any other reason. Fax it to (785) 339-2297.

| | | |
|---|---|---|
| 11. User's Name (Last, First, MI.) **(Please print)** | 12. Rank/Rate/Grade: | 13. Employee ID # (**Not SSN**) |

**14. Notice to User:** 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). *Authorization to access another United States Government computer system does not imply reinstatement of the authorization being revoked.*

Unit Attached to: _____

**Acknowledgment (**user's signature**):** ______________________________ **(Date):**___________________

| | |
|---|---|
| **15. Authorizing Official** *(Signature, **Typed or printed** name, Rank, Title and Phone Number):*<br>______________________________________________<br>Name, Rank, Title (e. g. PPC Branch Chief, CO/OIC, XO/XPO, By direction), Phone Number | 16 Date: |
| *16. Direct-Access Security Administrator* Signature: | 17. Date: |

Instructions:

- Fax the completed first page of the form to the Security Administrator at the number on the form.
- Retain the original form in the unit's files until the member departs the unit.
- When the member departs the unit, or access needs to be terminated for some other reason, have the user sign and date the *Revocation of Access Notice* section of the form. Fax the complete form (both pages) to the Security Administrator.
- Direct-Access termination should be part of your unit/division/branch/section checkout process