

# Sector Lake Michigan Reservist Welcome Aboard Package



[USCG Sector Lake Michigan](#)  
2420 S. Lincoln Memorial Drive  
Milwaukee, WI 53207

(414) 747-7100

Welcome to Sector Lake Michigan, and congratulations on your orders! We look forward to meeting you and promise you a challenging work.

Sector Lake Michigan in Milwaukee, Wisconsin is home to three Coast Guard units including Sector Lake Michigan, Station Milwaukee and Electronics Support Detachment Milwaukee. Sector Lake Michigan is home to approximately 91 Active duty and 47 Coast Guard Reserve members. Sector Lake Michigan is also home to the Sector Command Center which provides oversight and command and control of resources in the Sector's AOR, including Search and Rescue, Pollution Response, and Homeland Security.

This package is designed to help you become ready for your new assignment at Sector Lake Michigan. Your first responsibility is to become acquainted with Sector Lake Michigan. A check in list can be picked up at the Sector Personal Office from your YN.



## **Basic Information**

### **Checking In**

**You are expected to report aboard in the Service Dress Blue uniform.** Until you have access to enter through the gates, you may park in the visitor section in front of the building. A phone is located just inside the main entrance; if you need to be let into the building during working hours, you can reach the Sector Officer of the Day (OOD) by dialing 5555. Go first to the Servicing Personnel Office, located at the top of the stairs and to the right, where you will check in. The Servicing Personnel Office will be open during the Active duty workday hours, and drill weekends.

### **Work routine**

The Active duty working hours at Sector Lake Michigan are 0700 – 1530, Monday thru Friday. These are the same working hours on weekends for drilling Reservists, but may vary at your supervisor's discretion. Reservists at Sector Lake Michigan are expected to drill on the third weekend of each month.

### **Uniform of the Day**

Sector Lake Michigan's Uniform of the day is a properly worn Operational Dress Uniform (ODU); however alternate uniforms can be worn in accordance with the Coast Guard Uniforms Regulations.

### **Berthing**

If you reside outside of reasonable commuting distance (50 miles, approximately a one hour drive), contact MK1 Dillon at 414-747-7090, Reserves Forces Readiness Staff (RFRS), for a room in the barracks if one is available, 3 weeks before your drill. Hotel lodging may be arranged by the RFRS staff if a room is not available on base. You will be responsible for providing your own transportation to and from Sector Lake Michigan for drill weekends.

### **Galley**

Sector Lake Michigan's galley is located in the Station building. During weekdays, the galley offers breakfast from 0630-0700 and lunch from 1130-1215. The galley is open during each month's established Reserve weekend only, serving breakfast and lunch during the same hours. During all other weekends, the galley is closed. Dinner is not served in the Sector Lake Michigan galley except for special events. Microwaves are available in the duty rooms and the Exchange has a variety of food items available during its own business hours.

### **CG Exchange**

The Coast Guard Exchange is located on the lower level of the Sector building, just inside the first set of main doors. The Exchange carries a wide variety of uniform items, personal care supplies, snacks, meals, drinks, movies, and various gifts. The Exchange hours are M-F, 0930-1600, Saturday, 0900-1600, closed Sunday.

### **Exercise Facilities**

Sector Lake Michigan has a small gym on the first deck of the building. It offers cardio equipment, weight machines, and free weights. In addition, there are several YMCA locations and other facilities in the area.

### **DEERS/RAPIDS**

To update your military ID card or enroll a family member in DEERS, the nearest facility is the Naval Marine Core Reserve Center which is located directly across the street. These facilities are available by appointment only.

## **Reserve Information**

USCG Reserve information links, as well as contact information for the Sector RFRS Staff can be located at the Sector Lake Michigan web site under the Reserve tab.

[www.uscg.mil/d9/sectLakeMichigan/SLMReserve.asp](http://www.uscg.mil/d9/sectLakeMichigan/SLMReserve.asp)

## **Regular Training Requirements**

As a member of the Coast Guard Selected Reserve, you will be expected to maintain updated training and Readiness requirements through all-hands Reserve drills, in the online learning portal, and Medical appointments. Every Reservist should make a habit of checking his or her own status at every drill weekend by logging into CGBI (Coast Guard Business Intelligence) from a Coast Guard workstation.

**TASK:** Go to the following website to find which Readiness elements you need to complete: <http://cgbi.osc.uscg.mil/2.0/personal.cfm>. Items not marked with a green check on the 'Compliance' tab need immediate action.

**TASK:** Check in at the Medical office, which is located on the lower level at the south end of the hallway. Make sure your Medical record is present, and if you noted any items that were not up-to-date in CGBI, make arrangements with the HS to take care of them.

In addition to Medical Readiness, CGBI will also show you which training requirements you need to fulfill for the current period. Click on the Skills Tab, and the link called MT which will be followed by your completion percentage. Some of the training listed may be completed only through the all-hands training sessions with other Reservists; however, many of them must be done on your own through the online learning portal.

**TASK:** Establish a login for this website and familiarize yourself with its contents.

## **Readiness at Home**

There are many resources available for your Readiness preparation while away from drill weekends. You are expected to maintain communication with the Reserve force by checking your e-mail between drills, using your government identification card and a CAC reader. After the initial setup, the reader is easy to use and viewing e-mails via Outlook Web Access takes only a few minutes.

**TASK:** Make arrangements to get your CAC reader. Your reader comes with a CD and easy installation instructions. Make sure you have your Outlook Web Access established and ready *before* an urgent need arises, to avoid delays in communication.

**TASK:** Review the most current Reserve Quarterly Newsletter located on this site and identify opportunities to get acquainted with Sector Lake Michigan. Ask questions if you find anything that you aren't familiar with, and feel free to submit your own additions to the Editor!

Reservists at Sector Lake Michigan drill every month on the third weekend, unless otherwise specified for All Hands training purposes or by your supervisor. You are responsible for scheduling your drills in the Direct Access.

**TASK:** After receiving your Direct Access Login ID and Password, explore Direct Access and become familiar with the Help feature. Ask an experienced shipmate to navigate the site with you. Complete all of the following the first time you log in, to ensure the Coast Guard can reach you for recall or important information:

- Schedule your next drill. Include your supervisor's e-mail address so he/she is aware of the next time you are coming in.
- Enter your Coast Guard e-mail address and identify it as 'Business'. If you ever become locked out of Direct Access, this is the address where you can receive a reset password.
- Enter your other e-mail addresses (home, work, or school) where you can be reached outside of drill weekends.
- Enter your personal phone numbers, including mobile, work, and home.
- Make sure your home address is up-to-date.
- Find the Annual Screening Questionnaire location. You will be required to update this every year in the month of October.

Readiness Management Period (RMP) is a type of drill which can compensate a Reservist for certain authorized purposes such as maintaining medical, dental, and training Readiness. RMP's are scheduled using the same procedure as listed above, selecting RMP instead of IDT in Direct Access.

### **Security at Sector Lake Michigan**

All buildings at Sector Lake Michigan remain locked at all times and are accessible only by electronic key fob. This fob will also allow you entrance through the main gate

**TASK:** Make arrangements to visit with the EMC (Engineering Division) to receive your key fob. You will be required to sign a responsibility form and know where the key fob is at all times.

**If you ever lose your key fob**, whether on a drill weekend on base or away from Sector Lake Michigan, call the OOD immediately for direction to someone who will deactivate it.

When entering and leaving the gates on base, you are responsible for making sure the gate is secure behind you. When no Active duty member is standing watch on weekends or after hours, remain parked in your car after moving through the gate. Do not leave the area until you are sure the gate is closed and no one has entered the base unauthorized.

## **Contents of this Package and Getting Started Tasks**

The following important forms are provided in this Welcome Aboard Packet for you to fill out upon arrival. Please complete the following and return to the appropriate person as soon as possible. These pages also include tasks that will help you become ready for what Sector Lake Michigan expects of you as a Reservist. **Complete all items in this section during your first drill.**

### **Item Return Completed Form To:**

Welcome Aboard Checklist  
AIS Form for computer use

Department Supervisor  
ESD

**CG Sector Lake Michigan  
Reserve Welcome Aboard Check In**

**Full Name** \_\_\_\_\_ **Rate/Rank** \_\_\_\_\_ **Emp ID #** \_\_\_\_\_

*Meet with each of the following Members or departments during your first day to complete these items:*

**Command Cadre**

- \_\_\_ Sector Commander
- \_\_\_ Deputy Commander
- \_\_\_ Command Master Chief
- \_\_\_ Department Head
- \_\_\_ Division Head
- \_\_\_ RFRS

**Reserve Chain of Command**

- \_\_\_ SRO
- \_\_\_ Reserve Command Master Chief
- \_\_\_ Supervisor

**Administrative Division**

- \_\_\_ Update Direct Access Personal Info
- \_\_\_ Online Readiness Form
- \_\_\_ Annual Screening Questionnaire
- \_\_\_ Verify next marking period due date
- \_\_\_ Verify next OER due date
- \_\_\_ Confirm mobilization site location
- \_\_\_ Know mobilization qualifications
- \_\_\_ Mobilization prep-family/employer
- \_\_\_ Acknowledge Uniform Policy
- \_\_\_ Acknowledge Parking locations
- \_\_\_ Verify Weigh-In

**Medical Division**

- \_\_\_ Medical / Dental Record Drop Off
- \_\_\_ Verify Medical Readiness
  - PHA
  - Dental
  - Immunizations
  - Influenza
  - H1N1
  - Medical Tests

**Security**

- \_\_\_ Key FOB – Key Control Officer
- \_\_\_ Department Key - Supervisor
- \_\_\_ Security Clearance Check – OS1
- \_\_\_ Direct Access Account
- \_\_\_ Coast Guard Portal Account
- \_\_\_ AIS Form
- \_\_\_ Ensure Access to CG Intranet
- \_\_\_ Updated Emergency Notification System

**Education & Training**

- \_\_\_ Educational Service Officer
- \_\_\_ Sign Substance Abuse Statement
- \_\_\_ ADT Request
- \_\_\_ Review Mandated Training Status
  - \_\_\_ ICS 100
  - \_\_\_ ICS 200
  - \_\_\_ ICS 300
  - \_\_\_ ICS 400
  - \_\_\_ ICS 700
  - \_\_\_ ICS 800
  - \_\_\_ PHISH
- \_\_\_ Individual Development Plan (IDP)
- \_\_\_ Recommended Correspond. Courses
- \_\_\_ Coast Guard Institute website
- \_\_\_ SKILLSOFT

**Things To Do**

- \_\_\_ Keep daily journal of what you do related to the Coast Guard
- \_\_\_ Post resume on USCG website
- \_\_\_ Order CG business card if desired at 800-613-2803

**ESD**

- \_\_\_ Email
- \_\_\_ Acceptable Use Form

**AUTOMATED INFORMATION SYSTEMS (AIS)  
USER ACKNOWLEDGEMENT BRIEF  
(Version 1.0, 3 Feb 2009)**

**References**

- a. DHS MD 4300.1 (Series), Sensitive Systems Policy
- b. DHS MD 11042.1 (Series), Safeguarding Sensitive But Unclassified (For Official Use Only) Information
- c. COMDTINST M2000.3 (Series), Telecommunications Manual
- d. COMDTINST M4500.5 (Series), Property Management Manual
- e. COMDTINST M5260.3 (Series), The Coast Guard Freedom of Information (FOIA) and Privacy Acts Manual
- f. COMDTINST M5500.13 (Series), Information Assurance Manual
- g. COMDTINST M5510.23 (Series), Classified Information Management Program
- h. COMDTINST 2010.2 (Series), Use of Unclassified Wireless Devices, Services, and Technologies
- i. COMDTINST 5260.5 (Series), Privacy Incident Response, Notification, and Reporting Procedures for Personally Identifiable Information (PII)
- j. COMDTINST 5270.1 (Series), Management of Electronic Mail
- k. COMDTINST 5375.1 (Series), Limited Personal Use of Government Office Equipment

**Executive Summary**

This brief outlines Automated Information Systems guidelines for Government Information Systems, including, but not limited to the Coast Guard Data Network Plus (CGDN+) and Coast Guard Standard Workstation (CGSW), users. Each user shall adhere to all practices contained within this brief in order to safeguard against breaches of AIS security. Breaches of AIS security include, but are not limited to: Uncontrolled and unauthorized disclosure, alteration or destruction of Coast Guard information that could damage Coast Guard operations, personnel, or property. Breaches of AIS security may also lead to undue and unintentional embarrassment of Coast Guard.

**User Responsibilities**

**1. Official Use Policy:**

- Government Information Systems are governed by ref (k) and shall be used to conduct “Official Government Business.”
- Unauthorized access or use of government information systems is prohibited by Title 18, U. S. Code, Section 1030, Fraud and Related Activity in Connection with Computers.
- “Official Use” is defined by ref (k) as any activity that is conducted for the purpose of accomplishing official CG business.
- Limited “Personal Use” is defined by ref (k) as an activity that is conducted for purposes other than accomplishing official business, educational, or otherwise authorized activity.
- During Limited “Personal Use” time, all practices required during “Official Use” still apply to the user.

**2. Information Security:**

- Government Information Systems are considered SENSITIVE systems per ref (b); government information systems do process or have the potential to process protected information, including, but not limited to:
  - For Official Use Only (FOUO) as described in refs (a), (b), (c), and (f).
  - Privacy Act information or Personally Identifiable Information (PII) as described in ref (a), (e), and (i).
  - Privileged information related to the awarding of contracts.
  - Proprietary information that is the property of another organization or on loan to the government.
  - Financial data, such as budget, economical, management related data, and government credit cards.

**3. Physical Security:**

- Physical security of government information systems is a vital safeguard against unauthorized access and use, and can be achieved through basic measures identified in ref (a) and (b).

- All “Data At Rest” should be treated as For Official Use Only (FOUO) or Sensitive But Unclassified (SBU) and the storage device should be properly labeled and protected IAW ref (a), (b), (f), and ALCOAST 570/08 and 577/08.

#### **4. Network Security:**

- Network security is the means to protect the Government Information Systems and information contained within the CGDN+ and shall be achieved by performing security tasks including, but not limited to:
  - Per ALCOAST 570/08 and 577/08, ensure all files are virus scanned using an approved Anti-Virus application prior to being introduced to the CGDN+.
  - Personally owned PED, PC, etc. are not permitted to be physically attached to the CGDN+ at any time.
  - Remote Access Service (RAS) or Outlook Web Access (OWA) Anti-virus, Anti-spyware, and Endpoint monitoring software requirements are outlined in ALCOAST 032/09.

#### **5. Safeguarding Data:**

- An appropriate level of security shall be provided for all CG information.
- Print outs and other paper documents may contain SENSITIVE information should be stored iaw ref (b).
- The processing of classified information is strictly prohibited on unclassified CG resources.
- The processing of classified information on non-government-owned or non-accredited resources is a security violation and will result in the system being completely “scrubbed,” resulting in all data being lost or overwritten. There are NO EXCEPTIONS to this requirement.
- Incidents involving classified information shall be reported in accordance with ref (g).
- CG-Approved flash media devices (e.g. thumb drives) are identified within ALCOAST 516/08.
- Flash media devices have been suspended from directly connecting to the CGDN+ per ALCOAST 570/08 and 577/08. Mission essential applications that use flash media shall utilize the “air-gap” methods described in ALCOAST 570/08 and 577/08 to move data to/from the CGDN+.

#### **5. PASSWORDS or CAC PIN:**

- Every user of Coast Guard computer systems shall use a password or CAC PIN for access.
  - **PASSWORDS**
    - All passwords shall use be minimum of 14 ALPHANUMERIC, UPPER and LOWER CASE CHARACTERS, and a SPECIAL CHARACTER.
    - Passwords shall not be names/numbers that can easily be associated with you nor shall they be dictionary words.
    - Choose a password that is easy for you to remember but would be difficult to guess.
    - Do Not Share Your Password! The practices of sharing passwords and writing down passwords are prohibited. You are directly responsible for any misuse, abuse, or practices that may jeopardize the system that can be directly associated to your user name.
  - **CAC PIN**
    - All CAC PINs are composed of 6 to 8 numeric characters.
    - CAC PINs shall not be numbers or a combination of numbers that can easily be associated with you.
    - Do Not Share Your CAC or CAC PIN! The practice of sharing your CAC or CAC PIN is strictly prohibited.
- If you feel that your password or CAC PIN has become known or that unauthorized personnel are accessing your files or misusing the system, report it immediately to your supervisor, help desk, system administrator, or ISSO.

#### **6. ELECTRONIC MAIL:**

- Electronic Mail (E-mail) is described in ref (j).
- With the availability of gateways to public and private networks, E-mail transmitted for personal or unauthorized reasons has the potential to cause great embarrassment or harm to the Coast Guard.
- Government information systems shall not be used to support private or personal agendas, whether political, moral or philosophical per ref (j).
- DO NOT forward e-mail chain letters and jokes!

- Transmission of attachments greater than 10MB in CG e-mail negatively impacts network performance and IS NOT recommended (e.g. this practice degrades the performance of the overall system and will impact you and others).

**7. INTERNET MAIL:**

- Users must apply the criteria outlined in paragraph 2 to ensure SENSITIVE CG information IS NOT transmitted, received, or shared over the Internet due to the potential unauthorized access and viewing by recipients worldwide.
- Any e-mail containing FOUO, SBU, or sensitive information destined for outside the “uscg.mil” domain shall utilize encryption or password protection in order to protect the data in transit.
- “AUTOFORWARDING” your official CG E-mail to a personal or business Internet account IS STRICTLY PROHIBITED per ref (j).
- All users should be aware that any e-mail they send has the potential to be forwarded outside of the original intended distribution; dissemination to the Internet may also occur. All information shared in CG e-mail shall not be forwarded outside the “uscg.mil” without the expressed consent of the e-mail originator.
- Recipients should be aware of the originator’s desired intentions whether explicitly stated or not. COMMON SENSE AND SOUND JUDGEMENT SHOULD ALWAYS BE EXERCISED.

**8. COMPUTER VIRUSES/MALICIOUS PROGRAMS:**

- All CG-approved removable media shall be IMMEDIATELY scanned by virus detection software prior to being used on a government information system.
- Any software or files downloaded from bulletin boards or the Internet shall be scanned for viruses prior to being used on a government information system.
- All Remote Access CGSW users shall prevent the transmission of malicious programs, viruses, Trojans, etc. through the use of anti-virus software on the host resource.
- If you suspect you have loaded a virus, IMMEDIATELY contact your system administrator, help desk, or Information Systems Security Officer (ISSO). DO NOT ATTEMPT TO SOLVE THE PROBLEM ON YOU OWN (e.g. don’t delete, forward, or further process the file unless otherwise directed by a system administrator, help desk personnel, or ISSO.)

**9. ILLEGAL SOFTWARE, GAMES, AND BBS SYSTEMS:**

- In order to protect the integrity of CG information systems and their contents, the use or loading of illegal software (i.e. “bootleg,” pirated, or unauthorized copies), games, and “public domain” or third party software (shareware) is prohibited.
- Public domain software may be allowed if it has been certified and approved for use through the appropriate control board review process. The public domain software must perform a function that is not available through other available sources.
- It is illegal to reproduce or copy any licensed software or any copyright protected software the CG has purchased.
- Installation of any types of approved software shall ONLY be coordinated through your local system administrator or help desk. This may include a CG or contractor developed executable file.
- Unless specifically designed for and approved for CG use, copying and loading executable files to any CG owned or operated hardware is prohibited.

**10. GENERAL USE (Filing, Training, and Support):**

- Conduct a “cleanup” of your folders at least monthly. Files that may be needed for record purposes should be archived to CG-approved removable media and then deleted from your folder structure.
- It is the responsibility of each user to ensure he/she receives adequate training through your local support organization on the use of the CGSW, associated hardware, and the software operating within the device(s).
- Problems are an indication that something may be wrong with input, processing, or output operations and should be reported promptly to your system administrator or help desk for remediation.
- Whenever a problem or error occurs, immediately write down the error codes or message and a description of the work being done prior to the failure.

**11. PORTABLE ELECTRONIC DEVICES (PED):**

- ALL users of portable electronic devices (laptops, Palm devices, etc.) are responsible for all the provisions indicated above, in addition to the following:
  - Ensure the PED has all wireless capabilities disabled when connected to the CGDN+ wired network per ref (h).
  - Ensure the PED has an approved personal firewall, anti-virus software, and VPN client installed, is operational, and has the latest updates installed prior to disconnecting from and return to the CGDN+ wired network per ref (h).
  - Ensure the PED configuration is not modified with new hardware or software for connecting to wireless networks unless prior approval is received.
  - Know how to properly use and care for the PED, software, and associated peripherals while away from your unit.

### **12. USER CONSENT:**

By signing the AIS User Acknowledgement Form (CG-5500A), you acknowledge and consent that when you access Coast Guard information systems:

- 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 USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), 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, 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 an IS 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 AIS User Acknowledgement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any USG actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an IS, 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 PM, LE, or CI investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for PM, LE, or CI 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 policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an IS 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 privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and 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 policy. However, in such cases the USG 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 USG shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected from disclosure.
- In cases when the user has consented to content searching or monitoring of communications or data for PM, LE, or CI 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 USG may, solely at its discretion and in accordance with policy, elect to apply a privilege or other restriction on the USG's otherwise-authorized use or disclosure of such information.
- All of the above conditions apply regardless of whether the access or use of an IS 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 AIS User Acknowledgement, regardless of whether the banner describes these conditions in full detail or provide a summary of such conditions, and regardless of whether the banner expressly references this AIS User Acknowledgement.
- This AIS User Acknowledgement conforms to DoD CIO Memorandum, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent and User Agreement," May 9, 2008.

### **Conclusion**

- Upon completion of the AIS User Acknowledgement Brief, all users shall sign the AIS User Acknowledgement Form (CG-5500A) and process IAW local command policy.
- No user shall be granted access to the CGDN+ or any Government Information System prior to reviewing the AIS User Acknowledgement Brief and executing the AIS User Acknowledgement Form (CG-5500A).
- The AIS User Acknowledgement Brief and AIS User Acknowledgement Form (CG-5500A) shall be reviewed and signed each time a user transfers or relocates to a new unit.

U.S. DEPARTMENT OF  
HOMELAND SECURITY  
U.S. COAST GUARD  
CG-5500A (02-09)

## AUTOMATED INFORMATION SYSTEMS (AIS) USER ACKNOWLEDGEMENT FORM

User's Name ( <i>First, MI, Last</i> ) RANK/RATE	UNIT NAME	DIVISION/DEPT	ROOM NUMBER
Transferred? <input type="checkbox"/> YES <input type="checkbox"/> NO <i>(If YES, fill out block below)</i>	SUPERVISOR ( <i>or POC</i> )	PHONE NUMBER	
Transferred from What Unit? ( <i>Unit Name</i> )		FAX NUMBER	

### AUTHORIZATION TO ACCESS AUTOMATED INFORMATION SYSTEMS

#### SCOPE OF AUTHORIZATION

Subject to the limitation detailed in the Automated Information Systems User Acknowledgement Brief (and all applicable policies and regulations), this user is authorized access to U. S. Government information systems as required. This authorization contains no implied authorization to access any other information system of the U. S. Government not deemed necessary by user's supervisor or command. This authorization shall be revoked upon separation, retirement, reassignment of duties, change of organization, or when determined by the designated Coast Guard Security Representative to be in the best interest of the U. S. Government.

**WARNING: ONLY AUTHORIZED USERS MAY ACCESS U. S. GOVERNMENT INFORMATION SYSTEMS.** Individuals using U. S. Government information systems are subject to having all communications, data, and other activities monitored by U. S. Government personnel. Anyone using these systems expressly consents to monitoring activities as described in this brief and if such monitoring reveals possible evidence of misuse or criminal activity, said evidence may be provided to the appropriate U. S. Government entity for legal or punitive action.

#### ACKNOWLEDGEMENT

I understand that I am authorized access to U. S. Government information systems as necessary for the performance of my official duties. Access for purposes beyond the Scope of Authorization is a violation of Federal Law (Title 18 U.S.C. 1030 et wiu). I understand the AIS User Acknowledgement Brief along with my responsibilities to properly use and safeguard all U. S. Government information and resources. I understand that access to U. S. Government information systems may be revoked for failure to comply with the AIS User Acknowledgement brief and disciplinary actions may be taken for military members or civilian employees. I further understand that **THERE IS NO EXPECTATION OF PRIVACY WHILE USING U. S. GOVERNMENT INFORMATION SYSTEMS, THAT THE U. S. GOVERNMENT INFORMATION SYSTEMS ARE SUBJECT TO MONITORING, AND I AGREE TO ALL OTHER TERMS CONTAINED WITHIN THE AUTOMATED INFORMATION SYSTEMS USER ACKNOWLEDGEMENT BRIEF.**

Member Signature	Date
------------------	------

**Submit**

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

U.S. DEPARTMENT OF HOMELAND SECURITY U. S. Coast Guard CG-7421B (Rev. 02-11)		<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 #
4. Dept ID & Unit Name (Include Staff Symbol)	5. Area Code & Phone Number:		6. e-Mail address:
7. User Role Description (Note: See Chapter 1 of the <u>Personnel and Pay Procedures Manual, PPCINST M1000.2(series)</u> for an explanation of user roles common to field units). (Include current roles, this authorization supersedes all of your previous authorizations):			<b>Revocation:</b> Direct Access Roles are automatically terminated upon PCS, separation, retirement, reassignment of duties (Fleet-Ups) and change of organization (inter-office transfer).  CGHR SUP user roles for PAOs are automatically terminated each fiscal year unless the PAO completes annual required training and is re-designated in accordance with Chapter 1 of <u>CG SPO Manual, PPCINST M5231.3(series)</u>  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 due to reasons other than those listed above contact PPC Customer Care via on-line trouble-ticket at <a href="http://www.uscg.mil/ppc/ccb">http://www.uscg.mil/ppc/ccb</a> or <a href="http://cgweb.ppc.uscg.mil/ccb/">http://cgweb.ppc.uscg.mil/ccb/</a> or via email at <a href="mailto:PPC-DG-CustomerCare@uscg.mil">PPC-DG-CustomerCare@uscg.mil</a>
<input type="checkbox"/> CGSSCMD--Command User (evals, drills, Airport Terminal, etc.) <input type="checkbox"/> CGEMPREV -- Employee Review Only (not needed if you have CGSSCMD or CGHRS) <input type="checkbox"/> CGRSVDRL – Schedule, Edit and Approve Reserve IDT Drills (Only) <input type="checkbox"/> CGRSVMGR – Create, review, and endorse requests for reserve orders. <input type="checkbox"/> CGAIRTRM--Airport Terminal Only (Relocation Specialists/Housing Office) <input type="checkbox"/> CGFIELDADM--Unit with access to Member Competencies (Quals, Awards & Schools) (Route request through your Servicing Personnel Office – <u>Per Pay &amp; Personnel Procedures Manual, PPCINST M1000.2(series), Chap 1.</u> ) <input type="checkbox"/> CGGWIS--Global Workforce Inquiry System (Provides View Only Access to Personal Data) <input type="checkbox"/> CGHRS -- (SPO) DEPT ID _____ (See Chapter 1 of the <u>CG SPO Manual, PPCINST M5231.3(series)</u> for rules) <input type="checkbox"/> CGAPPL – Applicant Data (Use with CGHRS for accessions. This role is necessary to create applicant IDs. Cannot be selected with CGHR SUP.) <input type="checkbox"/> CGHR SUP—(SUPERVISOR, Payment Approving Official (PAO)) (Application must be approved by PPC (MAS)). (See Chapter 1 of the <u>CG SPO Manual, PPCINST M5231.3(series)</u> ) <input type="checkbox"/> CGSIPDR (SPO Access to the EI-PDR via WebNow - also complete form CG-7421D)			
PPC (MAS) PAO Designation Approved by (name/signature): _____ Date: _____			
<input type="checkbox"/> CGMRS — Medical Readiness System Clinical Access (Med care providers) <input type="checkbox"/> CGTRNOFF – Electronic Training Request (ETR). Unit ESOs. <input type="checkbox"/> CGFTESO – Unit Educational Services Officer. Unit ESOs. <input type="checkbox"/> CGSECURN--Unit Security Manager (View Only) <input type="checkbox"/> CGSECUVW--Area/Dist Security Manager (View Only). Fax completed form to COMDT (CG-86) at 202-372-3950 for approval. CG-86 will forward to PPC. CG-86 Name/Sign: _____ Date: _____			
<input type="checkbox"/> CGTRNFAC--Training Center (TAS Course Sessions) <input type="checkbox"/> CGTRNTQC--TQC/TAS Course Scheduler <input type="checkbox"/> CGASGN--CGPSC (epm/opm/rpm) or District/PSSU/BASE Reserve Assignment Officer <input type="checkbox"/> CGRSVISC/CGRSVORD—Reserve Orders Approval/Funding, District (r)/PSSUs only. <input type="checkbox"/> Others Not Listed. Please describe (in the space below) what you need to access in DA: _____			
8. Authorizing Official (Signature & Typed or printed name, Rank, Title ("By direction" is not authorized. Only the CO/OIC, XO/XPO or Division/Branch Chiefs at HQs/DCMS/CGPSC/PPC/FORCECOM/OPCOM (and their sub-units), Districts or Sectors may sign) & Phone Number: I certify that the access I have authorized is based on an official need. I am aware of the general functionality I have authorized and I am aware of what this will allow this member/employee to complete. If this is for a PAO Designation, I certify the member has completed online mandatory training requirements. If I have recommended an E5 be designated as a PAO, I have attached required justification. If this is for a contractor, the Contracting Officer's Technical Representative (COTR) signs as AO.			
Signature AND PRINTED or TYPED Name, and Rank		Title	9 Date:
Area Code & Phone (ext)		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.	
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) (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.)			
10. User's Signature:		11. Date:	Fax to: (785) 339-2297 (fax only page 1, do not fax instructions)