U.S. Department of Homeland Security
United States Coast Guard

Commander
United States Coast Guard
Personnel Service Center

US Coast Guard Stop 7200
4200 Wilson Blvd Suite 900
Arlington, VA 20598-7200
Staff symbol: PSC
Phone: (202) 872-6477

PSCINST 5200.1

MAR 7 2014

PERSONNEL SERVICE CENTER INSTRUCTION 5200.1

Subj: POLICY ON PROTECTION OF SENSITIVE AND PERSONALLY IDENTIFIABLE INFORMATION

Ref: (a) Coast Guard Freedom of Information & Privacy Acts Manual, COMDTINST M5260.3
(b) Safeguarding Sensitive But Unclassified (For Official Use Only) Information, DHS MD11042.1
(c) Coast Guard Public Affairs Manual, COMDTINST M5728.2
(d) Coast Guard Security and Information Assurance Manual, COMDTINST M5500.13C, Ch. 5
(e) Privacy Incident Response, Notification, And Reporting Procedures For Personally Identifiable Information (PII), COMDTINST 5260.5

1. PURPOSE. This instruction establishes policy on protection and proper use of sensitive but unclassified (i.e., For Official Use Only) information and safeguarding of Personally Identifiable Information (PII) for all divisions at the Personnel Service Center (PSC).

2. ACTION. Personnel assigned to PSC shall familiarize themselves with and follow this directive. All personnel reporting to any division within PSC shall review and sign the PSC Non-Disclosure Agreement (enclosure 1). The signed form shall be presented to the Human Resources and Administration Division where it will be scanned, retained electronically and discarded upon transfer of the each member.

3. DIRECTIVES AFFECTED. None

4. DISCUSSION. This directive prescribes policy for identification and protection of information compiled and utilized to execute official business at the Personnel Service Center. This policy supplements DHS and Coast Guard policy in references (a) through (e).

5. CONCEPT. PSC is a central point of collection, utilization and dissemination of highly sensitive PII and sensitive information for members throughout the Coast Guard. This includes but is not limited to results of boards and panels, e-resumes, service policy changes, medical deliberations, retirement/separation proceedings, personnel records, evaluations and other information only suitable for viewing by those with a need to know in the course of official service business. The loss or misuse of this type of information can result in substantial harm to service personnel, and PSC staff shall exercise the utmost professionalism and discretion managing all forms of sensitive information. The information and data, if disclosed to unauthorized sources, could violate the Privacy Act, and/or result in financial loss or adverse legal actions. Certain information may be disclosed under the guidance of the Freedom of Information Act (FOIA), but extreme care shall be taken to ensure any information released is done so according to applicable guidelines.

6. PRESUMPTION OF FOUO. PSC staff shall presume the substance of oral, electronic or hardcopy information used for official business are FOUO.

7. CRITICAL INFORMATION LIST. The PSC Critical Information List (CIL) includes all sensitive but unclassified information processed in the conduct of official business. It includes information including or related to:

a. PII of any active duty, retired, reserve, civilian, auxiliary or separated Coast Guard member.

b. Any information regarding assignments, e-resumes, medical history or determinations, separations, retirements, service history, evaluations, discharges, disciplinary proceedings, results or deliberations of boards and panels and service policy changes.

c. Any Command investigations, legal deliberations, processes or casework.

d. Any layout details, emergency response or security procedures for the Ballston Office Complex outside of what is public information.

8. PROTECTION OF CIL INFORMATION. To appropriately protect CIL information PSC personnel shall:

a. Only access, or attempt to access, personal information for which access is granted and there is an official "need to know."

b. Not divulge password(s) or share them with any others for any reason.

c. Not disclose any unauthorized data, employee information, or agency specific sensitive but unclassified information which could adversely affect the Coast Guard's interest or privacy to which individuals are entitled.

d. Not use, release, or disclose any sensitive but unclassified information, in any form whatsoever, to any person or entity other than authorized individuals without authorization from the appropriate chain of command. This stipulation includes premature release of any board/panel results and assignment decisions/results.

e. Protect PII in accordance with the provisions of the Privacy Act (PA) and other pertinent laws and regulations governing the confidentiality of privileged information, and only release information under established PA/FOIA guidelines.

f. Review and follow the guidelines for transmitting CIL information over electronic mail from reference (d).

g. Review and sign the attached PSC Non-Disclosure Agreement. (enclosure 1)

9. TRANSPORTATION OF SENSITIVE INFORMATION. Due to business imperatives, PSC personnel are permitted to transport PII/Sensitive Information to alternate work locations when authorized by their respective chains of command. The above provisions apply to all Coast Guard information resources whether individually controlled or shared, stand-alone or networked. They apply to all computers and communication facilities owned, leased, operated, or contracted by the Coast Guard. This includes networking devices, personal digital assistants, telephones, wireless devices, personal computers, workstations, mainframes, minicomputers and any associated peripherals and software, regardless of whether used for administration, research, or other purposes.

10. REPORTING. Any unauthorized use, release or disclosure of non-public information in violation of applicable standards shall be reported in accordance with references (d) and (e). For military members, failure to comply may result in adverse administrative or disciplinary action, including action under the Uniform Code of Military Justice (UCMJ). Additionally, the obligations and prohibitions contained in this policy and references (d) and (e) are also applicable to all civilian employees of the Coast Guard and violations of these policies may serve as grounds for disciplinary or administrative action.

11. RESPONSBILITIES. If you have any question regarding this policy, please seek guidance from your chain of command and the Command Security Officer.

12. RECORDS MANAGEMENT CONSIDERATIONS. This Notice was thoroughly reviewed during the directives clearance process and it was determined there are no further records scheduling requirements in accordance with Federal Records Act, 44 U.S.C. 3101 et seq., NARA requirements, and Information and Life Cycle Management Manual, COMDTINST M5212.12 (series). This policy does not have any significant or substantial change to existing records management requirements.

13. ENVIRONMENTAL ASPECT AND IMPACT CONSIDERATIONS. Environmental considerations were examined in the development of this instruction and have been determined to be non-applicable.

D. R. CALLAHAN
Commander, Personnel Service Center

Encl: (1) PSC Non-Disclosure Agreement

U.S. Department of Homeland Security
United States Coast Guard

Commander
United States Coast Guard
Personnel Service Center

US Coast Guard Stop 7200
4200 Wilson Blvd Suite 900
Arlington, VA 20598-7200
Staff symbol: HR&A
Phone: (202) 872-6413

5211

MEMORANDUM

From: PSC HR & A

To: {Mbr's Name/Signature} _____

Subj: PERSONNEL SERVICE CENTER NON-DISCLOSURE AGREEMENT

Ref: (a) Policy on protection of sensitive and personally identifiable information, PSCINST 5200.1 (series)

1. Personnel Service Center (PSC) is a central point of collection, utilization and dissemination of highly sensitive Personally Identifiable Information (PII) and sensitive information for members throughout the Coast Guard. This includes but is not limited to results of boards and panels, e-resumes, service policy changes, medical deliberations, retirement/separation proceedings, personnel records, evaluations and other information only suitable for viewing by those with a need to know in the course of official service business. The loss or misuse of this type of information could result in substantial harm to service personnel. Therefore, PSC staff must exercise the utmost professionalism and discretion managing all forms of sensitive information.

2. The following terms and conditions apply:

a. Only access, or attempt to access, personal information for which you are granted access authorization, have a "need to know", or require access to the information to perform your duties.

b. Do not disclose any confidential data, employee information, or agency specific sensitive but unclassified information which could adversely affect the Coast Guard's interest or privacy to which individuals are entitled.

c. Do not use, release, or disclose any sensitive but unclassified information, in any form to any person or entity other than authorized individuals without written authorization.

d. Protect PII in accordance with the provisions of the Privacy Act and other pertinent laws and regulations governing the confidentiality of privileged information. If you become aware of any improper use, release or disclosure of non-public information, you must advise the command as soon as possible.

e. Any unauthorized use, release or disclosure of non-public information in violation of applicable standards may subject you to appropriate adverse actions may result depending on the severity of the violation.

3. See reference (a) if you have any question regarding this agreement or seek guidance from your chain of command or PSC's Command Security Officer.

#