UNITED STATES MARINE CORPS
MARINE CORPS BASE
QUANTICO, VIRGINIA 22134-5001

IN REPLY REFER TO:
MCCSI 5211.1
B 379
NOV 2 6 2012

MARINE CORPS COMMUNITY SERVICES DIVISION INSTRUCTION 5211.1

From: Director
To: Distribution

Subj: STANDARD OPERATING PROCEDURES FOR PROTECTING PERSONAL IDENTIFIABLE INFORMATION (PII)

Ref: (a) SECNAVINST 5211.5E (DON Privacy Program)
(b) SECNAV M-5210.1 (Records Management Manual)
(c) Department of Homeland Security Privacy Office's Handbook for Safeguarding Sensitive PII of 19 Jan 11
(d) National Institute of Standards and Technology (Guide to Protecting the Confidentiality of Personally Identifiable Information)
(e) DoDI 1000.30 (Reduction of Social Security Number Use Within DoD)
(f) MCCS LOI 5239.1 (SOP for Activating and Terminating User Accounts)
(g) MCCS LOI 5239.2 (SOP for Accessing Restricted Areas)

Encl: (1) Privacy Act Data Cover Sheet (DD Form 2923, Sep 10)

1. Purpose. The purpose of this instruction is to provide guidance and procedures for collecting, handling, storing, and disposal of PII in accordance with references (a) through (g) and to ensure the systems and processes we employ safeguard this sensitive information.

2. Background. The protection of PII and the overall privacy information are concerns for both individuals whose personal information is at stake and for organizations that may be liable or have their reputations damaged should such PII be inappropriately accessed, used, or disclosed. The most common causes of loss/compromise of PII have been the loss or theft of laptop computers, thumb drives, and other portable removable media; material being erroneously posted to DoD web sites; documents being misplaced or stolen; emails with attachments being improperly forwarded; and documents placed into recycling and trash bins prior to being rendered unrecognizable (i.e., beyond reconstruction).

3. Definition(s):

a. Personal Identifiable Information (PII): PII is "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."

b. Privacy Act of 1974: The Privacy Act of 1974 is the foundation of public sector privacy law in the U.S. It applies only to Federal agencies and provides a statutory basis for the required use of Fair Information Practices. The Privacy Act pertains only to data maintained within a System of Records (SOR), which means any "group of records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." Record is defined broadly to include any item of information about an individual, both paper and electronic.

c. Security: Protecting PII through appropriate administrative, technical, and physical security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

4. Minimizing the Use, Collection, and Retention of PII. The practice of minimizing the use, collection and retention of PII is a basic privacy principle. By limiting PII collections to the least amount necessary in order for MCCS to conduct its mission and limit potential negative consequences in the event of a breach involving PII is paramount. PII collections should only be made where such collections are essential to meet the authorized business purpose and the mission of MCCS. This general concept is often abbreviated as the "minimum necessary" principle.

5. Use of the Social Security Number (SSN). The SSN has been used as a means to identify and authenticate individuals. However, the threat of identity theft has rendered this widespread use unacceptable, resulting in the requirement that all Federal agencies evaluate how the SSN is used and eliminate its unnecessary use as required by reference (e). The acceptable uses of the SSN are those that are provided by law,

require interoperability with organizations beyond DoD, or are required by operational necessities. Those systems, processes, or forms that claim "operational necessity" shall be closely scrutinized on the use and protection of the SSN. Use of the SSN includes the SSN in any form, including, but not limited to, truncated (last four digits), masked, partially masked, encrypted, or disguised SSNs. Activities that collect SSNs shall review all system processes and forms to ensure that SSNs are only being collected and used as authorized. Any such use of the SSN shall be reviewed for eliminating the use of the SSN whenever possible.

6. Training. It is vital to DoD that the collection, retention, storage use, and disposal of PII be handled appropriately, and only by individuals who are qualified to do so and have a "need to know." To ensure that all personnel are trained, it is required that prior to operating systems that contain or use PII, individuals be trained on appropriate handling. Properly completing and documenting this training is essential to reducing the chance of loss or breach of PII. The NAF Human Resources Training Department will ensure that documented initial and annual training is completed by all MCCS employees on Information Assurance (IA), Payment Card Industry (PCI) compliance, Privacy Act and PII.

7. Activating and Terminating MIS User Accounts. Reference (f) provides the standard operating procedures to ensure that Recreational Tracking (RECTRAC), Electronic Point of Sale (EPOS), Email and Network systems are only accessed by authorized and trained personnel.

8. Accessing Restricted Areas. Reference (g) provides the standard operating procedures for accessing restricted areas in order to prevent the unauthorized access of sensitive materials by personnel entering the Accounting Department, Management Information Systems (MIS) Department, and the Warehouse Retention area located in Bldg 3036.

9. Portable Media. Any laptop computer, mobile computing device or removable storage media that processes or stores a compilation of electronic records containing PII shall be restricted to DoD owned, leased or occupied workplaces. Storage of any form of PII is prohibited on personally owned laptop computers, mobile computing devices, and removable storage media. When compelling operational needs require removal from the workplace, the laptop computer, mobile computing device or removable storage media shall:

a. Be signed in and out with the Branch Director or Management Information Systems (MIS) Office.

b. Be configured to require certification based authentication for log on.

c. Be set to implement screen lock, with a specified period of inactivity not to exceed 15 minutes.

d. Have all PII stored on, created on, or written from laptop computers, mobile computing devices and removable storage media as applicable encrypted.

e. Laptop computers, mobile computing devices and data stored on removable storage media must be password protected.

10. Safeguarding PII. Every employee should exercise due care when handling all PII and all information they encounter in the course of their work. PII, however, requires special handling because of increased risk of harm to an individual if it is compromised. The following handling guidelines apply to all MCCS employees handling PII.

a. Collect PII only as Authorized

(1) Be sure that when you collect PII, you have the legal authority to do so and if necessary have a Privacy Act system of records notice (SORN) in place that describes the information.

(2) When collecting PII from patrons, do not create unapproved paper or electronic forms or processes to collect PII.

b. Limit Use of PII

(1) Only use PII for official purposes.

(2) Only access PII when you need to know that information in the performance of your official duties.

(3) Do not access or share PII for entertainment or any other purpose unless it is related to your mission need to know.

(4) Remember, that you must secure PII in a locked drawer, cabinet, cupboard, safe, or other secure container when you are not using it. Never leave PII unattended and unsecured.

(5) Do not browse files containing PII out of curiosity or for personal reasons.

c. Secure PII

(1) When you handle, process, transmit, and/or store PII, you should limit the potential for unauthorized disclosure. To do this, protect against "shoulder surfing," eavesdropping, or overhearing by anyone without the need to know the PII.

(2) Do not take PII home or to any non-work site, in either paper or electronic format, unless appropriately secured. PII in electronic form must be encrypted. Paper documents must be under the control of the employee or locked in a secure container when not in use. Personally owned computers may not be used to save, store, or host PII. Proper authorization from management must be obtained prior to removing any PII from the workplace.

(3) Physically secure PII (e.g., in a *locked* drawer, cabinet, or desk; in a safe; or in another locked container) when not in use or not otherwise under the control of a person with a need to know. PII may be stored in a space where access control measures are employed to prevent unauthorized access by members of the public or other persons without a need to know (e.g., a locked room or floor, or other space where access is controlled by a guard, cipher lock, or card reader), but the use of such measures is not a substitute for physically securing PII in a locked container when not in use. If a controlled environment cannot be obtained then a Privacy Act Data Cover Sheet (enclosure 1) must be placed on the PII documents.

(4) When sending an email that contains PII, you must encrypt the email prior to sending. The subject line of the email must begin with "FOUO" and the body of the email must contain the following statement: "For Official Use Only - privacy sensitive (FOUO). Any misuse or unauthorized access may result in both civil and criminal penalties."

(5) Do not leave PII unattended on a desk, network printer, fax machine, or copier. Do not send PII to a fax machine without contacting the recipient to arrange for its receipt. When faxing PII, the document cover letter must state "FOUO" in the subject line with "For Official Use Only. Any misuse or unauthorized access may result in both civil and criminal penalties" in the body. When printing PII, verify the

printer location. Promptly pick up all copies of the copied document.

(6) Store PII in shared access computer drives ("shared drives") only if access is restricted to those with a need to know by permissions settings or passwords.

(7) Physically secure PII when in transit. Do not mail or courier PII on CDs, DVDs, hard drives, flash drives, USB drives, floppy disks, or other removable media unless the data is encrypted. Do not return failed hard drives to vendor for warranty if the device was ever used to store PII, but sanitize or destroy the media. For example, do not pack laptops or electronic storage devices in checked baggage. Do not leave them in a car overnight or in plain sight in a parking lot.

11. Disposal of Documents Containing PII

a. Records retention and disposal standards are provided in reference (b). Printed material can be destroyed using an approved cross-cut shredder, burn bags, or equivalent destruction means. Do not use recycle bins for this purpose and never discard PII documents in a trash bin.

b. Remember to secure PII that has been discarded in burn bags that are awaiting removal, shredding, or destruction.

c. Mobile devices containing PII must be sanitized according to MIS's standards when no longer needed by an employee.

12. Loss or Misuse of PII

a. Any loss or misuse of PII must be reported immediately to the activity's Director. The Director is responsible for complying with the requirements set forth in reference (a).

b. Employees not adhereing to the guidelines set forth in references (a) through (g) and this instruction may be subject to criminal and civil penalties and/or discliplinary actions up to and including termination.

13. Action

a. MCCS Directors, Managers, and Supervisors shall ensure that all employees under their cognizance have been trained and understand the contents of this instruction.

b. Upon receipt of this instruction and annually thereafter Directors, Managers and Supervisors are required to review their activity's procedures for collecting and utilizing PII, the use of forms that collect PII, the storage, security, and retention of information that contains PII. This includes the physical security of the activity (the locking of doors, windows, filing cabinets) and all access keys are secured and properly accounted for. In activities that collect SSNs the Directors, Managers and Supervisors shall review all system processes and forms to ensure that SSNs are only being collected and used as authorized. Any such use of the SSN shall be reviewed for eliminating the use of the SSN whenever possible.

c. All MCCS employees need to be constantly aware of the nature and importance of PII, collect only what we absolutely need, and take care that we handle, safeguard, and dispose of PII properly. Just as we do not tolerate loss of classified information, we cannot tolerate the loss of PII.

d. Although we cannot control all events that may cause a loss of PII, we can improve our internal controls over the handling and disposal of PII, as well as, better train and educate our employees.

M. L. HICKS

Distribution List: A