DEPARTMENT OF THE NAVY
OFFICE OF THE JUDGE ADVOCATE GENERAL
WASHINGTON NAVY YARD
1322 PATTERSON AVENUE SE SUITE 3000
WASHINGTON DC 20374-5066

IN REPLY REFER TO

JAG/CNLSCINST 5211.11
Code 13
JUN 14 2013

JAG/COMNAVLEGSVCCOM INSTRUCTION 5211.11

From: Judge Advocate General
Commander, Naval Legal Service Command

Subj: STANDARDS AND POLICY FOR SAFEGUARDING PERSONALLY IDENTIFIABLE INFORMATION

Ref: (a) DoDD 5400.11 (series)
(b) SECNAVINST 5211.5 (series)
(c) JAGINST 5720.3 (series)
(d) DON CIO MSG DTG 171625Z Feb 12
(e) DON CIO MSG DTG 081745Z Nov 12
(f) DODI 1000.30 (series)
(g) DON CIO MSG DTG 171952Z Apr 07
(h) DON CIO MSG DTG 281759Z Aug 12
(i) SECNAV M-5210.1 (series)
(j) DON CIO MSG DTG 291652Z Feb 08
(k) DON CIO MSG DTG 181905Z Dec 08
(l) ALNAV 042232Z Oct 07

1. Purpose. In accordance with references (a) through (l), to define clear standards for safeguarding personally identifiable information (PII) in the Office of the Judge Advocate General (OJAG) and Naval Legal Service Command (NLSC).

2. This is a new instruction and should be read in its entirety. Specific requirements for handling PII in the course of OJAG and NLSC telework are set forth in JAGINST 12620.

3. Background. Per reference (a), PII is defined as information which can be used to distinguish or trace an individual's identity. Examples include but are not limited to: name, social security number, date and place of birth, mother's maiden name, biometric records, financial records, and any other personal information linked or linkable to a specified individual. In our practice, Sailors, Marines, and civilians routinely entrust us with PII and it is our responsibility to ensure that the systems and processes we employ safeguard this sensitive information. To that end, this instruction provides guidance on

properly safeguarding, storing, transmitting, and destroying PII.

4. Applicability. This instruction applies to all military and civilian personnel assigned within OJAG and NLSC and to reserve units supporting OJAG and NLSC.

5. Policy. The JAG Corps community is committed to safeguarding PII by ensuring proper systems and processes are in place by every activity and/or command when making decisions involving the collection, use, sharing, retention, disclosure, and destruction of PII, whether in paper or electronic format.

a. Collection and Use of Social Security Numbers (SSNs). Pursuant to reference (f), all OJAG and NLSC personnel shall reduce or eliminate the use of SSNs wherever possible. Use of the SSN includes the SSN in any form, including, but not limited to, truncated, masked, partially masked, encrypted, or disguised SSNs. SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria defined in reference (f). Activities and/or commands should explore whether SSNs can be substituted with the Department of Defense (DoD) Identification (ID) number when possible. The DoD ID number is also considered PII and may not be shared with other Federal Agencies without a memorandum of understanding on the subject approved by the DON Chief Information Officer (CIO). Internal forms created by an activity and/or command that do not have an official Department of Defense (DoD) or Department of the Navy (DON) form number and are not related to a system of records must remove the use of SSNs.

(1) SSNs may be used in approved forms and systems when they meet one or more of the acceptable use criteria in reference (f). Examples of when the use of SSNs is permissible under the acceptable use criteria as defined in reference (f) include but are not limited to:

(a) The use of SSNs on charge sheets is permissible under the law enforcement acceptable use category as defined in reference (f);

(b) The use of SSNs is permissible on all NAVPERS forms containing a SSN requirement, including but not limited to, NAVPERS 1626/7 (NJP Report Chits), NAVPERS 1910/31 and 1910/32 (Administrative Separation notifications) as well as Administrative Separation Letters of Transmittal in accordance

with guidance from Commander, Navy Personnel Command (PERS 8), NAVPERS 1070/613 (Page 13), NAVPERS 1616/26 or 1616/27 (Evaluation Report and Counseling Records), and NAVPERS 1610/2 (Fitness Report and Counseling Records); and

(c) Defense Service Office, Legal Assistance, and Claim forms may still require a SSN if the form is covered by a System of Records Notice.

b. Marking of Records. Properly marking records with the appropriate document designation is important in order to protect sensitive, critical information from unauthorized release. In order to protect such information, it is imperative that a record be appropriately designated from the moment it is created.

(1) The individual who creates the record has the responsibility for properly marking the record. To determine the appropriate marking of a record, the creator should consider the purpose of the record, any exemptions under the Freedom of Information Act (FOIA), 5 U.S.C. § 552, and whether any personal information protected by the Privacy Act (PA), 5 U.S.C. § 552a, is contained therein. See reference (b) for guidance on OJAG FOIA and PA policies and procedures.

(2) "For Official Use Only (FOUO)" serves as a record designation, not a classification. All electronic or paper copy records containing PII data shall be properly marked as "FOR OFFICIAL USE ONLY - PRIVACY SENSITIVE - Any misuse or unauthorized disclosure of this information may result in both civil and criminal penalties." Use the PA Cover Sheet (DD Form 2923) when transporting records containing PII.

c. Transmitting PII. The PA strictly limits access to PII within an agency to those that have an official need-to-know. Where transmittal of PII is necessary, the originator must properly mark the correspondence to ensure the receiver of the information is aware of the need to properly protect it. The most secure methods for sending PII remain: (1) personal delivery, (2) encrypted e-mail, or (3) U.S. Postal System or other approved shipping carrier. In accordance with references (b), (d), (e), (g), and (h), the following guidelines shall apply:

(1) Electronic mail (e-mail) - E-mails containing PII must be properly marked "FOR OFFICIAL USE ONLY - PRIVACY SENSITIVE" in the subject-line of the e-mail. The following

shall be placed in the body of the e-mail: "FOR OFFICIAL USE ONLY-PRIVACY SENSITIVE: Any misuse or unauthorized disclosure of this information may result in both criminal and civil penalties." The e-mail must be digitally signed and encrypted. If a recipient is unable to receive encrypted e-mail, remove that recipient from the distribution and transmit the PII in an alternate manner provided within this instruction. At no time should PII be sent unencrypted. Receipt of PII from a non-DON source is not a violation of this instruction or the above-listed references. However, once in receipt of PII from a non-DON source, activities and/or commands shall not electronically forward that information without proper encryption.

(2) Faxing. Pursuant to reference (d), faxing of PII is prohibited. Commands are encouraged to utilize alternate methods of transmitting PII such as encrypted e-mail or the Safe File Exchange (SAFE) website. Reference (e) provides exceptions to this rule. Commanding Officers and Division Directors are authorized to approve exceptions and may delegate this authority to any civilian deputy or any officer in the pay grade of O-4, or higher.

(3) U.S. Mail. Precaution should be taken when sending PII via U.S. mail or other approved shipping carriers. A best practice is to double wrap the information prior to sealing the outer envelope. Ensure that the mailing label has the name and address of the correct recipient.

(4) SAFE. DON CIO has approved the use of Safe Access File Exchange (SAFE) as a method for sending unclassified materials, including files containing FOUO information and PII, to .mil and .gov domains. DON CIO has also approved the use of SAFE for transmission of PII to commercial e-mail addresses, such as .com or .edu. SAFE may be accessed online at: https://safe/amrdec.army.mil. Although SAFE messages are encrypted on the upload and download side, the SAFE notification e-mail message to the recipient (which includes the SAFE package link and a password) is not encrypted. While SAFE is authorized for transmitting PII, OJAG and NLSC personnel and reservists supporting OJAG and NLSC commands may not store records containing PII on personal devices. See paragraph 5(e) below.

(d) Transporting PII. Current guidance for removing PII from the workplace is found in references (b) and (g). When transporting PII between activities and/or commands, or when teleworking, documents removed from government workspaces shall be properly secured in envelopes or folders with a PA Data Cover

Sheet (DD Form 2923) affixed to the front. Documents shall be secured at the alternate work location in a manner consistent with this instruction. Pursuant to reference (g), when removing PII stored on DoD-owned equipment, the device must:

(1) Be signed in and out with a supervising official, designated in writing by the Commanding Officer or Division Director;

(2) Be configured to require certificate-based authentication for log-on;

(3) Be set to implement a screen lock, with a specified period of inactivity not to exceed 15 minutes; and

(4) Encrypt all PII stored, created, or written from the laptop computer, mobile computing devices, and removable storage media, as applicable. This applies only to PII stored on the computer itself and not documents or files stored on a network share drive accessible from the laptop.

(e) Storing PII. Pursuant to reference (g), the storage of any form of PII is prohibited on personally owned laptop computers, mobile computing devices, and removable storage media. Documents containing PII maintained on network drives should only be accessible by those with a need-to-know and should be properly marked.

(f) Disposal of PII. PII shall be disposed of in accordance with references (b), (h) and (i). Pursuant to reference (b), disposal of documents containing PII is considered adequate if the records are rendered unrecognizable or beyond reconstruction (e.g., shredding or destroying in a burn bag). Electronic storage media and information systems containing PII shall be disposed of in accordance with the requirements in reference (h).

6. PII Breach Reporting. Personnel who have discovered a known or suspected loss of PII must report the breach to their supervisor. Activities and/or commands shall designate, in writing, an officer responsible for reporting PII breaches and to serve as the point-of-contact (POC) for follow-up actions and individual notifications. This individual may be the same person designated as the activity or command PA coordinator per reference (c).

(a) For purposes of this instruction, the term breach includes the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users, for other than an authorized purpose, have access or potential access to PII, whether physical or electronic. This includes transmittal of PII without employing the safeguards discussed above.

(b) Pursuant to reference (j), within one hour of discovery of a loss or suspected compromise or loss of PII, a breach report shall be filed electronically at www.doncio.navy.mil/Main.aspx. The electronic breach report is automatically sent to the DON CIO Privacy Team via a list serve which includes OJAG Code 13 as a recipient. An activity or command in receipt of improperly transmitted PII is responsible for contacting the sending activity or command to facilitate the submission of a breach report. The activity or command which may have committed a breach is responsible for submitting the breach report.

(1) Within 24-hours, the DON CIO Privacy Team will review the initial breach report and determine the potential risk of harm to impacted personnel. Based upon this review, the DON CIO Privacy Team will notify the organization's designated official of follow-up reporting requirements and if notifications are required. The reporting command is required to forward DON CIO's response to Code 13 at OJAG_PII_BREACH@navy.mil.

(c) Defense Counsel Assistance Program Director, Defense Service Offices (DSOs), Trial Counsel Assistance Program Director, and Region Legal Service Offices (RLSOs) shall make a voice report to the Chief of Staff for DSOs or RLSOs, whichever is applicable, within one hour of discovery of a loss or suspected compromise of PII. Naval Justice School shall make a voice report to CNLSC. Division Directors shall make a voice report to the cognizant Assistant Judge Advocate General.

(d) Code 13 shall track reported breaches by OJAG divisions and NLSC commands for compliance and trends.

7. Training. In accordance with references (k) and (l), all personnel shall complete annual training on safeguarding PII by August 31st of each year. The training is available on Navy Knowledge Online. Division Directors, Commanding Officers, and Executive Officers shall ensure that the requirements of this

instruction are part of the check-in process for newly reporting personnel.

8. Semi-annual Spot Checks. In accordance with reference (1), all OJAG and NLSC commands shall perform a semi-annual PII spot check. Code 13 shall provide notice and guidance for the semi-annual spot check. Employing these spot checks and taking aggressive corrective action where deficiencies have been identified are keys to a successful privacy program and ensure compliance with this instruction.

a. The designated local PII Coordinator shall conduct a spot check of their assigned areas of responsibility, focusing on those areas where the compromise of PII is most likely to occur (e.g., copy machines, fax machines, PII undestroyed in garbage receptacles, printers, etc.).

b. A checklist located at www.doncio.navy.mil/main.aspx shall be utilized to conduct the spot checks. Activities and/or commands shall maintain this checklist for their records. Upon completion of the spot check, each activity and/or command shall report completion to Code 13. It is not necessary to forward the checklist to Code 13.

9. Effective Date. This instruction is effective immediately.

10. POC. Code 13 is the POC for all matters relating to this instruction and may be reached at (703) 693-2606, DSN 223-2606.

J. W. CRAWFORD III
Commander, Naval Legal Service Command

NANETTE M. DeRENZI
Judge Advocate General