

(CORRECTED) MCBUL 5239. INTERIM GUIDANCE FOR HANDLING, /SAFEGUARDING AND REPORTING BREACHES OF PERSONALLY IDENTIFIABLE/INFORMATION (PII)

Date Signed: 9/4/2008

MARADMIN Number: 491/08

R 031636z SEPT 08

MARADMIN 491/08

MSGID/GENADMIN/CMC WASHINGTON DC//

SUBJ/(CORRECTED) MCBUL 5239. INTERIM GUIDANCE FOR HANDLING, /SAFEGUARDING AND REPORTING BREACHES OF PERSONALLY IDENTIFIABLE /INFORMATION (PII)//

REF/A/MSGID:GENADMIN/DON CIO WASHINGTON DC/171952ZAPR2007//

REF/B/MSGID:MARADMIN/CMC WASHINGTON DC C4/142229ZDEC2007//

REF/C/MSGID:MARADMIN/CMC WASHINGTON DC C4/262120ZJUL2006//

REF/D/MSGID:DOC/MC IA OPERATIONAL STANDARD 10 /YMD:20060920//

REF/E/MSGID:DOC/SECNAV M-5210.1/-//

REF/F/MSGID:DOC/SECNAV M-5214.1/-//

REF/G/MSGID:DOC/MCO 3504.2/-//

REF/H/MSGID:DOC/DOD 5400.11-R/-//

NARR/REF A IS DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER DIRECTIVE ON SAFEGUARDING PII. REF B IS MARADMIN 732/07 PROVIDING THE POLICY FOR DATA AT REST ENCRYPTION FOR MOBILE COMPUTING DEVICES AND REMOVABLE STORAGE MEDIA. REF C IS MARADMIN 348/06 PROVIDING POLICY FOR THE USE OF DATA PROTECTED BY THE PRIVACY ACT. REF D IS MARINE CORPS INFORMATION ASSURANCE OPERATION STANDARD 010 UNAUTHORIZED DISCLOSURE AND ELECTRONIC SPILLAGE HANDLING. REF E IS SECNAV M-5210.1 DEPARTMENT OF THE NAVY, RECORDS MANAGEMENT PROGRAM, RECORDS MANAGEMENT MANUAL. REF F IS DEPARTMENT OF THE NAVY INFORMATION REQUIREMENTS (REPORTS) MANUAL. REF G IS OPERATIONS EVENT/INCIDENT REPORT (OPREP-3) REPORTING DIRECTIVE. REF H IS DEPARTMENT OF DEFENSE PRIVACY PROGRAM DIRECTIVE.

REPORT REQUIRED: BREACH AND COMPROMISE REPORT (REPORT CONTROL SYMBOL EXEMPT) PAR. 4.C.//

POC/JOSEPH S UCHYTIL/MAJ/UNIT:HQMC C4 IA/-/TEL:703-693-3490

/EMAIL:JOSEPH.UCHYTIL@USMC.MIL//

POC/TIMOTHY LISKO/CTR/UNIT:HQMC C4 IA/-/TEL:703-693-3490

/EMAIL:TIMOTHY.LISKO.CTR@USMC.MIL//

GENTEXT/REMARKS/1. PURPOSE. THIS BULLETIN CONSOLIDATES PREVIOUS POLICY REGARDING PII.

2. CANCELLATION. THIS MESSAGE SUPERCEDES AND CANCELS MARADMINS 742/07, 431/07, 389/07 AND 267/07.

3. BACKGROUND. PII IS DEFINED AS INFORMATION WHICH CAN BE USED TO UNIQUELY AND RELIABLY IDENTIFY AN INDIVIDUAL. THIS INFORMATION CAN INCLUDE NAME, DATE OF BIRTH (DOB), SOCIAL SECURITY NUMBER (SSN), ADDRESSES, TELEPHONE NUMBERS, EMAIL ADDRESSES, MOTHERS MAIDEN NAME, FINANCIAL, CREDIT, AND MEDICAL DATA, AMONG OTHERS. RECURRING BREACHES AND LOSSES OF PII HAVE LED TO A GROWING CONCERN AMONG THE PUBLIC REGARDING THE PROPER SAFEGUARDING AND HANDLING OF THEIR PERSONAL INFORMATION. PUBLIC TRUST IN THE MARINE CORPS COULD POTENTIALLY ERODE IF PROPER STEPS ARE NOT TAKEN TO PROTECT PII. THE MARINE CORPS UNDERSTANDS THAT PROPER EDUCATION AND TRAINING REGARDING THE PROTECTION OF PII SERVES TO REDUCE FUTURE INSTANCES OF PRIVACY BREACHES. FURTHERMORE, ADVANCES IN TECHNOLOGY AND CHANGES IN

PCN 10207718300

DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

LAWS, REQUIREMENTS, AND REGULATIONS REQUIRES THE MARINE CORPS TO REMAIN FLEXIBLE AND ABLE TO ADAPT TO AN EVER CHANGING ENVIRONMENT BY CONTINUOUSLY UPDATING AND/OR CHANGING POLICY FOR PII.

4. ACTION

A. SAFEGUARDING PII

(1) ALL SYSTEMS AND APPLICATIONS COLLECTING, STORING, OR DISSEMINATING PII MUST HAVE AN APPROVED PRIVACY IMPACT ASSESSMENT (PIA) ON FILE WITH THE DEPARTMENT OF THE NAVY, CHIEF INFORMATION OFFICER (DON CIO) PRIOR TO OPERATION. THIS INCLUDES BOTH PROGRAMS OF RECORD (POR) AND LOCALLY CREATED SYSTEMS.

(2) ANY DOCUMENT CONTAINING PII WILL BE MARKED FOR OFFICIAL USE ONLY (FOUO) ON EACH PAGE.

(3) ANY PII STORED ON NETWORK RESOURCES/DEVICES IN SHARED FOLDERS SHALL BE, AT MINIMUM, PASSWORD PROTECTED, AND SHALL ONLY BE AVAILABLE TO THOSE INDIVIDUALS WITH AN AUTHORIZED BUSINESS NEED TO KNOW. PII WILL NOT BE STORED IN PUBLIC FOLDERS OR ANY OTHER FOLDERS/LOCATIONS WITH UNRESTRICTED ACCESS.

(4) PII RECORDS SHALL BE MAINTAINED IN ACCORDANCE WITH THE APPROPRIATE STANDARD SUBJECT IDENTIFICATION CODE (SSIC) CONTAINED IN REF E.

(5) PII SHALL NOT BE MAINTAINED ON PERSONALLY OWNED COMPUTERS/DEVICES. PII WILL ONLY BE MAINTAINED ON DOD OWNED, CONTRACTED OR LEASED ASSETS.

(6) EMAIL, TO INCLUDE ATTACHMENTS, CONTAINING ANY AMOUNT OF PII MUST BE DIGITALLY SIGNED AND ENCRYPTED USING DOD APPROVED CERTIFICATES. FOUO WILL BE INCLUDED AT THE BEGINNING OF THE SUBJECT LINE. THE BODY OF THE EMAIL SHALL CONTAIN A STATEMENT NOTIFYING THE RECIPIENT TO TREAT THE EMAIL AND ITS CONTENTS AS FOR OFFICIAL USE ONLY-PRIVACY SENSITIVE (FOUO). ANY MISUSE OR UNAUTHORIZED ACCESS MAY RESULT IN BOTH CIVIL AND CRIMINAL PENALTIES.

(7) PII CREATED, MAINTAINED OR MANIPULATED ON ANY MOBILE DEVICE (I.E. BLACKBERRY, FLASH DRIVE, EXTERNAL HARD DRIVE, CELL PHONE, ETC.), MUST BE ENCRYPTED THROUGH CURRENTLY APPROVED METHODS. SHOULD ENCRYPTION NOT BE AVAILABLE, PII WILL NOT BE CREATED, MAINTAINED OR MANIPULATED ON THE DEVICE.

(8) PII WILL BE RESTRICTED TO DOD OWNED, LEASED OR OCCUPIED WORKSPACES. 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 A SUPERVISING OFFICIAL DESIGNATED IN WRITING BY THE COMMAND.

(B) BE CONFIGURED TO REQUIRE CERTIFICATE BASED AUTHENTICATION FOR LOG ON (FOR LAPTOP COMPUTERS AND MOBILE COMPUTING DEVICES WHERE POSSIBLE).

(C) BE SET TO IMPLEMENT SCREEN LOCK, WITH A SPECIFIED PERIOD OF INACTIVITY NOT TO EXCEED 15 MINUTES (FOR LAPTOP COMPUTERS AND MOBILE COMPUTING DEVICES WHERE POSSIBLE).

B. DISPOSAL AND DESTRUCTION. DISPOSAL METHODS FOR PAPER DOCUMENTS CONTAINING PII IS ADEQUATE IF THE INFORMATION IS LEFT BEYOND RECONSTRUCTION I.E., CROSS-CUT SHREDDING, BURNING, OR CHEMICAL DECOMPOSITION. DOCUMENTS CONTAINING PII SHALL NOT BE DISPOSED OF IN TRASH CANS OR RECYCLING CONTAINERS UNLESS PROPERLY SHREDDED.

DESTRUCTION METHODS FOR PII ON ELECTRONIC STORAGE DEVICES E.G., COMPUTER HARD DRIVES, IAW REF C, IS DEFINED AS ANY PROCEDURE THAT RENDERS IT UNREADABLE AND UNUSABLE. METHODS TO ACHIEVE THIS INCLUDE

DEGAUSSING, OVERWRITING, OR DESTROYING THE DEVICE.

C. BREACH AND COMPROMISE REPORTING. WITHIN ONE HOUR OF DISCOVERY OF ACTUAL OR SUSPECTED LOSS, THEFT, OR COMPROMISE OF PII, THE COMMAND WILL ASSEMBLE AND COMPLETE ALL INFORMATION SPECIFIED ON THE PII COMPROMISE REPORT TEMPLATE LOCATED ON THE MARINE CORPS PII WEBSITE, [HTTPS:\(SLASH SLASH\) HQDOD.HQMC.USMC.MIL/PII.ASP](https://(SLASH SLASH) HQDOD.HQMC.USMC.MIL/PII.ASP) AND REPORT THE INFORMATION TO THE BELOW OFFICES AND AGENCIES. PRIMARY MEANS SHALL BE A SINGLE EMAIL. IF ACCESS TO EMAIL IS NOT AVAILABLE COMMANDS SHALL REPORT VIA TELEPHONE. THIS REPORTING REQUIREMENT IS EXEMPT FROM REPORTS CONTROL IN ACCORDANCE WITH REFERENCE F, PT IV, PAR. 7.G.

(1) UNITED STATES COMPUTER EMERGENCY READINESS TEAM (US-CERT),
EMAIL: SOC@US-CERT.GOV. TEL: 888-282-0870

(2) DON CHIEF INFORMATION OFFICER (CIO) IDENTITY MANAGEMENT AND PRIVACY TEAM, EMAIL: DON.PRIVACY.FCT@NAVY.MIL. TEL: 703-601-0120/6882.

(3) DON PRIVACY ACT OFFICER, EMAIL: PRIVACY@OGC.LAW.NAVY.MIL.
TEL: 202-685-6545.

(4) MARINE CORPS CIO, HQMC C4 IA, IDENTITY MANAGEMENT (IDM) TEAM,
EMAIL: HQMC_C4IA_IDMGT@USMC.MIL. TEL: (703) 693-3490.

(5) HQMC PUBLIC AFFAIRS MEDIA BRANCH (PAM), EMAIL:
M_HQMC_PA_MEDIARELATIONS@USMC.MIL. TEL: 703-614-8029.

(6) MARINE CORPS PRIVACY OFFICER, EMAIL:
SMBHQMCPRIVACYACT@USMC.MIL. TEL: 703-614-4008.

(7) LOCAL NAVAL CRIMINAL INVESTIGATIVE SERVICE (NCIS) OFFICE OR MARINE CORPS INVESTIGATION DIVISION (CID).

(8) LOCAL STAFF JUDGE ADVOCATE (SJA) OFFICE

(9) MARINE CORPS NETWORK OPERATIONS AND SECURITY COMMAND (MCNOSC) WATCH OFFICER, EMAIL: MCNOSCWO@MCNOSC.USMC.MIL. TEL: 703-784-5300.

MARINE CORPS UNITS ARE REQUIRED TO ISSUE A NAVAL MESSAGE TO THE DOD ORGANIZATIONS OUTLINED ABOVE WITHIN 72 HOURS OF THE INITIAL REPORT. THE MESSAGE WILL CONTAIN, AT A MINIMUM, ALL INFORMATION PROVIDED IN THE ORIGINAL EMAIL. PLAIN LANGUAGE ADDRESSES (PLADS) FOR ORGANIZATIONS ARE: DON CIO WASHINGTON DC, OGC WASHINGTON DC, CMC WASHINGTON DC C4 IA, CMC WASHINGTON DC PA, ACC QUANTICO CWO, AND CMC WASHINGTON DC AR. MARINE CORPS UNITS ASSIGNED TO COMBATANT COMMANDS OR UNDER THE OPERATIONAL CONTROL OF COMBINED OR JOINT FORCE COMMANDER WILL ADDITIONALLY ISSUE AN OPREP-3SIR. COPIES OF ALL PII COMPROMISE OPREP-3SIR WILL BE SUBMITTED TO THE USMC PRIVACY OFFICER AS A FOLLOW UP TO THE INITIAL REPORT OF THE COMPROMISE. THIS REPORTING REQUIREMENT IS IN ACCORDANCE WITH REFERENCE G. ALL FOLLOW UP ACTIONS REQUIRED BY THE REPORTING COMMAND WILL BE COORDINATED THROUGH THE USMC PRIVACY OFFICER AT SMBHQMCPRIVACYACT@USMC.MIL. WITHIN 24 HOURS OF INITIAL REPORT, COMMANDS WILL SUBMIT THE FOLLOWING INFORMATION VIA EMAIL TO THE DISTRIBUTION LIST OUTLINED ABOVE:

(A) REPORT OF THE STATUS OF THE COMMANDS PLAN TO NOTIFY INDIVIDUALS WHOSE INFORMATION WAS COMPROMISED.

(B) DESCRIPTION OF ACTIONS BEING TAKEN TO PREVENT FUTURE OCCURANCES WITHIN 10 DAYS OF INITIAL DISCOVERY OF A KNOWN OR SUSPECTED COMPROMISE, AND ON THE DIRECTION OF HQMC, THE COMMAND WILL NOTIFY THE AFFECTED PERSONNEL OF THE LOSS. AT A MINIMUM THE NOTIFICATION SHALL INCLUDE SPECIFIC PII INVOLVED; CIRCUMSTANCES SURROUNDING THE COMPROMISE; AND PROTECTIVE MEASURES THE INDIVIDUAL CAN TAKE. NOTIFICATION SHALL BE MADE IN ONE OR A COMBINATION OF THE FOLLOWING FORMS: LETTER, DIGITALLY SIGNED EMAIL, TOLL-FREE NUMBER CALL CENTER FOLLOWING GUIDELINES LOCATED AT [HTTP:\(SLASH\)\(SLASH\)PRIVACY.NAVY.MIL](http://(SLASH)(SLASH)PRIVACY.NAVY.MIL)

UNDER ADMINISTRATIVE TOOLS, OR A GENERALIZED NOTICE TO THE POTENTIALLY AFFECTED POPULATION WHEN THE COMMAND CANNOT READILY IDENTIFY THE AFFECTED INDIVIDUALS. IF THE COMMAND CANNOT PROVIDE NOTIFICATION WITHIN THE 10 DAY PERIOD, A REPORT MUST BE SUBMITTED TO THE USMC PRIVACY OFFICER (SMBHQMCPRIVACYACT@USMC.MIL) AND HQMC C4 IA IDM TEAM PROVIDING JUSTIFICATION FOR THE DELAY, AND A PLAN OF ACTION AND MILESTONES (POA&M) OUTLINING THE STEPS TAKEN TO COMPLETE THE PROCESS. REPORT LESSONS LEARNED VIA EMAIL WITHIN 10 DAYS OF THE INCIDENT TO THE USMC PRIVACY OFFICER AND HQMC C4 IA IDM TEAM. (C) COMMANDS WILL REPORT ACTUAL LOSS OR THEFT OF PII RECORDS AND DATA TO CMC (ARDB). PROCEDURES FOR THE REPORT OF ACTUAL LOSS OR THEFT OF PII RECORDS AND DATA ARE CONTAINED IN PARAGRAPH 6 OF REF (E).

D. TRAINING. COMMANDS WILL ENSURE THAT ALL INDIVIDUALS (MARINES, CIVILIANS, AND CONTRACTORS) COMPLETE ANNUAL DEFENSE INFORMATION SYSTEMS AGENCY (DISA) PII TRAINING AND THAT AUDITABLE RECORDS ARE RETAINED FOR THE CURRENT CALENDAR YEAR FOR VERIFICATION OF TRAINING.

COMMANDS ALSO HAVE THE OPTION TO DIRECT THEIR STAFF TO TAKE SUPPLEMENTAL TRAINING TO ENHANCE THEIR KNOWLEDGE OF PII. ALL TRAINING MODULES AND CERTIFICATES ARE LOCATED ON THE MARINE CORPS PII WEBSITE. DEPLOYING UNITS MAY DEFER ANNUAL TRAINING AND CERTIFICATION 60 DAYS PRIOR TO DEPARTING CONUS AND 60 DAYS UPON RETURN TO CONUS.

E. COMPLIANCE. COMMANDS WILL ENSURE THAT ALL SUBORDINATE LEADERSHIP AND MANAGEMENT CONDUCT BI-ANNUAL REVIEWS FOR COMPLIANCE IN THE HANDLING, STORAGE, AND DESTRUCTION OF PII WITHIN THEIR AREA(S) OF RESPONSIBILITY. COMMANDS WILL USE THE PII COMPLIANCE CHECKLIST LOCATED ON THE MARINE CORPS PII WEBSITE. AS AN AUDITABLE DOCUMENT, CHECKLISTS WILL BE KEPT ON FILE BY THE COMMAND FOR THREE YEARS.

F. REPORTING. COMMAND INFORMATION ASSURANCE MANAGERS WILL REPORT COMPLETION OF ANNUAL TRAINING AND COMPLIANCE REVIEWS NLT 21 DECEMBER OF EACH YEAR USING THE REPORT TEMPLATE ON THE MARINE CORPS PII WEBSITE. ALL REPORTS WILL BE MADE VIA CHAIN OF COMMAND WITH MARFORS, MCCDC AND HQMC DEPARTMENTS CONSOLIDATING SUBORDINATE REPORTS AND SUBMITTING TO HQMC C4 IA AT HQMC_C4IA_IDMGT@USMC.MIL. THIS REPORTING REQUIREMENT IS IN ACCORANCE WITH REFERENCE H, CHAPTER 8.

5. COMMANDS WILL ENSURE THE IMPLEMENTATION OF THIS POLICY WITHOUT DELAY AND DISSEMINATE THROUGH THE WIDEST MEANS, INCLUDING POSTING ON ORGANIZATIONAL BULLETIN BOARDS.

6. RESERVE APPLICABILITY. THIS BULLETIN IS APPLICABLE TO THE MARINE CORPS TOTAL FORCE AND CONTRACTORS IN SUPPORT OF THE MARINE CORPS.

7. CANCELLATION CONTINGENCY. THIS BULLETIN, UNLESS SUPERCEDED, IS CANCELLED 2 JULY 2009.

8. RELEASE AUTHORIZED BY BGEN G. J. ALLEN, DIRECTOR, COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTERS/CHIEF INFORMATION OFFICER OF THE MARINE CORPS.//