DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
3000 MARINE CORPS PENTAGON
WASHINGTON DC 20350-3000

MCO 5211.5
AR (ARSF)
28 Aug 2024

MARINE CORPS ORDER 5211.5

From: Commandant of the Marine Corps
To: Distribution List

Subj: UNITED STATES MARINE CORPS (USMC) PRIVACY PROGRAM

Ref: See enclosure (1)

Encl: (1) References
(2) Headquarters Marine Corps (HQMC) Staff Offices/Commands and Subordinate Commands with Privacy Coordinators
(3) Sample Privacy Coordinator Designation Letter (for Privacy Coordinator or Privacy Point of Contact (POC))

Reports Required: I. Section 803 Report, par. 3b(1)(b)23, par. 3b(5)(i), and par. 3b(5)(q)
II. Federal Information Security Modernization Act (FISMA) Report, par. 3b(1)(b)23, and par. 3b(5)(q)

1. Situation. This Order reinstates and updates the implementing instruction for the United States Marine Corps (USMC) Privacy Program. It assigns responsibilities to ensure compliance with references (a) through (ah) and relevant laws and regulations. Detailed guidance and specific procedures for addressing these requirements will be issued separately and made available on the USMC Privacy Program SharePoint Site at: https://usmc.sharepoint-mil.us/sites/AR_HQMC_PA.

a. Reference (b) requires the establishment of an implementing instruction and the designation of Privacy Coordinators to serve as principal points of contact (POCs) on Privacy Program matters to ensure compliance with the Privacy Act (reference (a)), the Department of the Navy (DON) Privacy Program Instruction (reference (b)), and relevant laws and regulations.

b. This Order reflects existing policy and procedures and incorporates new regulatory requirements associated with the administration and oversight of the USMC Privacy Program. It does not create any rights, privileges, or benefits, substantive or procedural, enforceable by any party against the United States, its departments, agencies, other entities, its officers, or any other persons. In the event of a conflict between this Order and any existing USMC directive or policy, this Order supersedes.

c. This Order is in accordance with references (a) through (ah).

2. Mission. To issue a Marine Corps Order (MCO) for the USMC Privacy Program to meet the requirement to have an implementing instruction in accordance with reference (b).

3. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent. Reinstate and update the USMC Privacy Program implementing instruction to meet current requirements and assign responsibilities for execution.

(2) Concept of Operations

(a) Designation of the USMC Privacy Program Manager and USMC Privacy Program Coordinator;

(b) Designation of the USMC Breach Reporting Officer;

(c) Delegation of responsibilities for implementing the DON Privacy Program requirements within USMC, including designation of Privacy Coordinators and Privacy POCs; and

(d) Establishment of USMC-specific requirements and responsibilities for complying with references (a) and (b), relevant privacy laws and regulations (including personally identifiable information (PII) breach reporting procedures), and Office of Management and Budget (OMB) policies.

b. Subordinate Element Missions

(1) Headquarters Marine Corps (HQMC), Freedom of Information and Privacy Acts Office (ARSF). The Head of the Freedom of Information and Privacy Acts Office (ARSF) is designated as the USMC Privacy Program Manager. ARSF serves as the principal advisor to the Commandant of the Marine Corps (CMC), Headquarters Marine Corps (HQMC) staff agencies, and the Fleet Marine Force on all Privacy Program matters. ARSF issues policy/guidance, provides administrative support and advice, conducts training, and monitors overall USMC Privacy Program effectiveness. ARSF is responsible for ensuring the implementation of the DON Privacy Program requirements within USMC. ARSF will ensure that all USMC military members, civilians, and contractor employees (USMC personnel) are fully aware of their rights and responsibilities under the Privacy Act (PA), and that the USMC's need to maintain information to meet mission requirements is balanced against the obligation to protect individuals against unwarranted invasions of their privacy stemming from the collection, maintenance, use, and disclosure of PII. Implementation of program requirements is the responsibility of the USMC Privacy Program Coordinator, under the direct supervision of the USMC Privacy Program Manager. ARSF is responsible for the following:

(a) Head, Freedom of Information and Privacy Acts Office (ARSF). ARSF oversees the Marine Corps Privacy Program and shall designate an individual to serve as the USMC Privacy Program Coordinator for the Marine Corps.

(b) United States Marine Corps (USMC) Privacy Program Coordinator

1. Administers the Marine Corps Privacy Program, including execution of the Privacy Act in accordance with references (a) and (b) and relevant privacy laws, regulations, and guidance requirements within the Marine Corps.

2. Issues and maintains this Order to define program requirements, assign responsibilities, and implement the USMC Privacy Program.

3. Serves as the Marine Corps Privacy liaison and coordinates interactions between the Marine Corps, Department of the Navy Chief Information Officer (DON CIO), Navy Privacy Office (DNS-H (36)), Department of Defense (DoD) component Privacy offices, and the Office of the Assistant to

the Secretary of Defense for Privacy, Civil Liberties, and Transparency (ATSD-PCLT).

4. Maintains a list of the Marine Corps Privacy Coordinators and POCs, to include name, command, and contact information (work email address and phone number).

5. Provides guidance to Marine Corps Privacy Coordinators, Privacy POCs, and USMC personnel regarding all aspects of the USMC Privacy Program, including but not limited to the requirements of the PA and relevant privacy laws and regulations; maintenance and protection of PII; identifying and reporting breaches; DON Social Security Number (SSN) Reduction Plan; handling PA requests and complaints; scope of PA exemptions; and training requirements.

6. Conducts staff assistance visits and/or program evaluations when requested by the command, including at least one Major Subordinate Command (MSC) annually, to ensure compliance with the references.

7. Develops Marine Corps Privacy education, training and awareness resources and ensures that Marine Corps personnel, contractors, PA System Managers, Privacy Coordinators, and Privacy POCs have access to and receive appropriate training regarding the collection, handling, maintenance, and disclosure of PII.

8. Maintains the USMC Privacy Program website (https://www.hqmc.marines.mil/Agencies/USMC-FOIA/USMC-Privacy-Act/) and SharePoint site (https://usmc.sharepoint-mil.us/sites/AR_HQMC_PA).

9. Develops, updates, and posts procedure guides to the Privacy Program SharePoint site for use by all USMC Privacy Coordinators, POCs, PA System Managers, and personnel for implementing Privacy Program requirements. At a minimum, guides will be posted for:

a. Breach Reporting.

b. Compliance Spot Checks and Inspections.

c. Privacy Act Complaints.

d. Privacy Act Requests.

e. Privacy Act Statements.

f. Privacy Impact Assessments.

g. System of Records Notices (SORNs).

h. Training.

10. Coordinates with the Administration and Resource Management Division (AR), Publishing and Logistics Management Branch (ARD), Records, Reports, Directives, and Forms Management Section (ARDB) officers, the Command, Control, Communications, and Computers Division (IC4) Privacy Impact Assessment (PIA) coordinator and USMC Breach Reporting Officer, PA System Managers, Privacy Coordinators, and Privacy POCs to ensure compliance with the references.

11. Reviews Marine Corps orders, bulletins, forms, practices, and procedures for PA implications and, where PII is solicited, used, or maintained, ensures compliance with the references.

12. In coordination with ARDB, ensures all PA systems of records are kept in accordance with retention and disposal requirements.

13. Reviews and approves Marine Corps SORNs, coordinates the establishment, revision, and deletion of Marine Corps SORNs (to include joint Navy and Marine Corps SORNs for which Marine Corps is the lead sponsor) and ensures they are reviewed annually. In addition, coordinates review for proposed DoD-wide SORNs when tasked by Privacy, Civil Liberties, and Transparency (PCLT).

14. Ensures Marine Corps offices and commands conduct annual reviews of their PA systems of records to ensure that they are necessary, accurate and complete and that no official files are maintained on individuals without first ensuring that a SORN exists that permits such collection.

15. Develops and maintains an Inspector General (IG) functional area checklist for Privacy meeting Inspector General of the Marine Corps (IGMC) inspection checklist standards and provides support for inspections when requested.

16. Conducts internal PII compliance spot-check inspections at least twice annually and ensures that internal assessments are conducted by all offices and commands.

17. Coordinates with IC4 to ensure that all Marine Corps Information Technology (IT) systems and applications that maintain PII have a PIA completed and approved in accordance with reference (h) prior to the collection of PII.

18. Reviews and validates Marine Corps PIAs for compliance with Privacy Program requirements and provides the validation to IC4 and DON CIO.

19. Coordinates with USMC Breach Reporting Officer at IC4 and/or DON CIO to ensure immediate action is taken to report the actual or suspected loss of control, unauthorized disclosure, or unauthorized access of PII (breach) and that appropriate follow-up actions are taken as directed by the USMC Breach Reporting Officer and/or DON CIO Breach Reporting Officer. Should a loss occur, ensures that affected individuals have access to resources and guidance for the protection of their identity.

20. Ensures that the DON SSN Reduction Plan is implemented in accordance with reference (g) and DoD policy.

21. Processes PA requests.

22. Coordinates PA complaints. Ensures complaints are directed to the correct office or command for action and that final action is reported to ARSF.

23. Provides USMC input to DON CIO for inclusion in the annual Federal Information Security Modernization Act (FISMA) Report, Section 803 Report, and other reports as required.

24. Represents the Marine Corps at PCLT meetings and DON CIO Privacy and Breach Response Team (BRT) meetings.

(2) Deputy Commandant for Information (DC I). The Deputy Commandant for Information (DC I) serves as the USMC Chief Information Officer (CIO) to the CMC. To align the Marine Corps with the DON Breach Reporting/Responding Process and DON PIA reviewing/approving process, DC I will support the USMC Privacy Program by designating a USMC Breach Reporting Officer

and assigning responsibilities as described by this Order, and by ensuring all Marine Corps IT systems and applications that collect, maintain, use, or disseminate PII are in compliance with reference (h).

(a) Command, Control, Communications, and Computers Division (IC4). Performs the duties of the USMC Breach Reporting Officer as assigned by DC I.

(b) United States Marine Corps (USMC) Breach Reporting Officer. Coordinates with ARSF to:

1. Supervise USMC execution of the PII Breach Reporting/Responding process per reference(f), to include:

a. Receiving and reviewing all USMC reports of suspected or confirmed PII breaches.

b. Performing risk assessments and providing determinations and instructions for all required follow-up actions (to include notification when appropriate).

c. Coordinating with designated USMC, DON CIO, and DoD Privacy officials as necessary to conclude USMC PII breach incidents.

d. Should a major breach occur, participating as part of the DON BRT in accordance with reference (f).

2. Receive, review, and enter PIAs into the DON PIA Reviewing/Approving process.

3. Provide instruction as required to ensure uniform and coordinated service implementation of federal, DoD and DON directed policies for safeguarding PII.

(3) Inspector General of the Marine Corps (IGMC). IGMC Inspections Division inspects all major commands that are required to execute a Commanding General's Inspection Program (CGIP) for compliance with Critical or Required Evaluation (CoRE) functional areas. IGMC provides inspection checklist standards to facilitate the development and maintenance of functional area checklists by the program sponsors and notifies the policy owner on an annual basis to review/update the IG checklist as appropriate.

(4) Headquarters Marine Corps (HQMC) Staff Offices and Major Subordinate Commands (MSCs)

(a) Administer and oversee implementation of the USMC Privacy Program within their individual staff office or MSC and their subordinate commands/units, to include the execution of the requirements in references (a) and (b), relevant privacy laws, regulations, and this Order.

(b) Establish command-specific procedures to meet Privacy Program requirements and assign responsibilities, to include identifying the placement within the organization of the Privacy Coordinator and subordinate command/unit Privacy POCs.

(c) Designate, in writing, a Privacy Coordinator to serve as the principal point of contact for Privacy matters and provide a copy of the designation letter and contact information to ARSF. Enclosure (2) lists the HQMC staff offices and MSCs that are required to designate a Privacy Coordinator. The list also includes several subordinate commands that have been determined to require a Privacy Coordinator because of their structure and/or the nature of their specific mission requirements.

(d) Determine whether each individual subordinate command/unit should have a designated Privacy Coordinator or Privacy POC based on its size and needs (e.g., quantity and sensitivity of PII maintained). Each office/command has broad discretion on the placement and designation of their Privacy Coordinators and POCs. However, if a subordinate command/unit is not required to have their own Privacy Coordinator/POC, the Privacy Coordinator/POC at the next senior level within the reporting chain must also serve that function for the subordinate command/unit to ensure that Privacy Program requirements are met.

(e) HQMC staff offices not listed in enclosure (2) may designate either a Privacy Coordinator or a Privacy POC based on the needs of the office.

NOTE: The Office of Personnel Management (OPM) created the Government Information Specialist job series, 0306, in March 2012. This series includes both Freedom of Information Act (FOIA) and Privacy professionals. Individuals recruited to fill full-time positions as Privacy Coordinators should be hired under series 0306. Those fulfilling these responsibilities on a

part-time or sporadic basis may remain under the designated job series for their primary job responsibilities.

(f) Notify ARSF of the appointment of new Privacy Coordinators and POCs. Provide designation letters for Privacy Coordinators and a complete list of Privacy POCs with contact information.

(g) Ensure that designated Privacy Coordinators, Privacy POCs, PA System Managers, and personnel who routinely handle large quantities and/or highly sensitive PII (to include contractors) receive adequate training. Training must cover program requirements and the office's/command's specific needs involving the collection and maintenance of PII. The annual Privacy/PII training required for all personnel only covers basic requirements and is insufficient for these individuals.

(h) Any HQMC staff office or MSC created as a result of changes to USMC organizational structure and not currently listed in enclosure (2) will be required to meet the provisions of this Order.

(5) Privacy Coordinators

(a) Serve as the principal point of contact on Privacy matters for the office/command and ensure that the collection, use, storage, dissemination and/or disclosure of PII complies with the references and relevant privacy laws, regulations, and this Order.

(b) Maintain a current list of Privacy POCs, to include name, title, and contact information, for the office/command and subordinate commands/units and provide a complete list and any updates, as needed, to ARSF.

(c) Provide guidance to all office/command personnel on Privacy Program requirements, including, but not limited to, maintenance and protection of records containing PII, identifying and reporting breaches, identification, review and completion of compliance documents (SORNs, PIAs, etc.), handling of PA requests and complaints, DON SSN Reduction Plan, and training requirements.

(d) Coordinate with ARSF, ARDB, IC4, local records, reports, directives, and forms officers, PA System Managers, and Privacy POCs to provide program support for their organization and ensure compliance with the references and this Order.

(e) Ensure that subordinate command/unit Privacy POCs, PA System Managers, and personnel who routinely handle large quantities and/or highly sensitive PII (to include contractors) are properly trained regarding collecting, handling, maintaining, and disseminating PII. Training must cover program requirements and the office's/command's specific needs involving the collection and maintenance of PII. The annual Privacy/PII training required for all personnel only covers basic requirements and is insufficient for these individuals.

(f) Review internal directives, forms, practices, and procedures to ensure those having PA implications and/or where PII is used or solicited are in compliance with the PA and program requirements.

(g) Conduct assistance visits or program evaluations to ensure compliance with the PA and program requirements.

(h) Process PA requests.

(i) Process PA complaints. PA complaints should be processed at the lowest appropriate level. The office/command shall investigate any PA complaint received involving the office/command or a subordinate command/unit when it is determined that the subordinate command/unit cannot or should not do so. The office will implement any appropriate corrective actions required to resolve the specific issue and to prevent any future occurrences. A copy of the investigation report and final command actions taken will be provided to ARSF for inclusion in the Section 803 Report within ten business days after completion.

(j) Ensure appropriate safeguards and controls are in place to avoid unauthorized access to or loss of PII.

(k) Take immediate action to report the actual or possible loss of control, unauthorized disclosure, or unauthorized access of PII (breach). Should a loss occur, take appropriate actions as directed by the USMC and/or DON CIO Breach Reporting Officer, to include notifying affected individuals if directed to do so, apprising them of how to ascertain whether their privacy/identity has been compromised, and directing them to resources providing assistance for victims of identity theft, if needed.

(l) Ensure the office/command and subordinate commands/units conduct annual reviews of their PA systems of records to ensure that they are necessary, accurate and complete.

(m) Ensure no official files are maintained on individuals without first ensuring that a SORN exists that permits such collection.

(n) Ensure that the SORNs relied upon by the office/command are reviewed at least once a year, report completion of the reviews to ARSF (per references (b) and (d)) and advise ARSF promptly of the need to establish, revise, or delete a SORN.

(o) Coordinate PIAs for office/command information systems with the appropriate stakeholders, review and validate the PIAs, and ensure the validated PIAs are submitted to IC4 for review and coordination.

(p) Conduct internal PII compliance spot check inspections/assessments at least twice annually, ensure that internal assessments are conducted by their subordinate commands/units, and track and provide completion summaries to ARSF at the end of the fiscal year (per references (b) and (d)). Compliance spot check reports are auditable records and shall be maintained by the command in accordance with record schedule 5000-82 of reference (i). Commands may use the USMC IG inspection checklist for Privacy, the sample spot check form available on USMC Privacy Program SharePoint site, or the sample compliance spot check forms available on the (at: https://www.doncio.navy.mil/TagResults.aspx?ID=36). Follow DON CIO guidance for using these sample forms.

(q) Provide input to ARSF for inclusion in the annual FISMA Report, Section 803 Report, and other reports as required.

(r) Provide review and comment for proposed SORNs and other Privacy Program documents when tasked by ARSF, and task reviews to subordinate command/unit POCs, as needed.

(6) Privacy Points of Contact (POCs). Privacy POCs serve as the point of contact on Privacy Program matters for their command/unit and ensure that the collection, use, storage, dissemination and/or disclosure of PII by the command/unit is in compliance with the references and this Order. Privacy POCs

have the same responsibilities as Privacy Coordinators but will generally participate at a lower level in the chain of command and with guidance and direction from their MSC's Privacy Coordinator and/or next senior level Privacy POC. POCs perform program responsibilities as-needed and usually on a part-time or sporadic basis. At a minimum, they must be able to:

(a) Work closely with their MSC Privacy Coordinator and/or next senior level Privacy POC to ensure compliance with the references and this Order.

(b) Provide guidance to personnel within their command/unit on Privacy Program requirements pertaining to maintenance and protection of command/unit records containing PII, identifying and reporting breaches, and where to obtain additional guidance and support.

(c) Take immediate action to report the actual or possible loss of control, unauthorized disclosure, or unauthorized access of PII (breach). Should a loss occur, take appropriate actions as directed by the USMC and/or DON CIO Breach Reporting Officer, notify affected individuals if directed to do so and direct them to resources providing information on how to determine if their privacy/identity has been compromised and/or assistance for victims of identity theft, if needed.

(d) Conduct internal PII compliance spot check inspections at least twice annually, and track and report completions to their MSC Privacy Coordinator. Compliance spot check reports are auditable records and shall be maintained for three years.

(7) Privacy Act (PA) System Managers

(a) Serve as the official responsible for overseeing the collection, maintenance, use, and dissemination of information from a PA system of records, regardless of format (paper or electronic). Each system of records has a designated System Manager.

(b) Ensure that only those personnel with an official need to know have access to the records maintained in the system and are aware of their responsibilities for protecting the PII maintained in them.

(c) Ensure appropriate administrative, technical, and physical safeguards are in place for the protection of the system of records for which they are responsible.

(d) Ensure that all records containing PII (paper and electronic) are properly marked to identify the records as potentially requiring special consideration for maintenance, handling, and dissemination. Documents containing PII shall be marked in accordance with Controlled Unclassified Information (CUI) requirements per reference (k). The DoD CUI Registry, policy and guidance for markings are available at https://www.dodcui.mil.

(e) Ensure that, if an individual is asked to provide personal information (name, date of birth, SSN (full or any portion thereof), DoD ID number, etc.), regardless of the method used to collect the information (e.g., enters own information into an IT system or paper form, personal or telephonic interview, etc.) to be included in the system of records, a Privacy Act Statement (PAS) is provided to the individual. The statement enables the individual to make an informed decision regarding whether or not to provide the information requested. If information is requested only to confirm identity or retrieve a record, a modified Privacy Act advisory statement may be provided instead.

NOTE: If the information is not requested from the individual (e.g., is pulled from another system or entered by a third party without consulting the individual), neither a PAS nor an advisory statement is required. Only a Privacy Warning statement/CUI marking is required on the document or in the system containing the PII.

(f) Ensure the privacy of the individuals and the confidentiality of PII contained in the PA system of records and protect the records from reasonably anticipated threats or hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to the individual about whom the information pertains. Information contained in the PA system of records shall not be disclosed by any means to any person, or to another agency, except pursuant to a written request by or with the prior written consent of the individual to whom the record pertains unless it is pursuant to one of the exceptions included in the PA.

(g) Ensure all disclosures of information made without the consent of the record subject, except those made within DoD in the performance of official duties or under FOIA, are accurately recorded and the disclosure accounting is maintained with the applicable records. While not required by statute, it is recommended that all disclosures be included in the accounting record.

(h) Ensure that no official files that contain PII are maintained in the system of records unless/until a SORN exists that permits such collection.

(i) Coordinate with the office/command Privacy Coordinator/POC to complete a PIA and identify or initiate a new SORN as required for all new and existing systems that maintain PII.

(j) Review the SORN(s) for the systems of records under their cognizance annually to ensure the SORN(s) accurately reflects the system and the information maintained. Advise the office/command Privacy Coordinator/POC promptly of the need to establish, revise, or delete a SORN.

(k) Take reasonable steps to ensure the accuracy, relevance, timeliness, and completeness of all records maintained in the system of records.

(l) Ensure all records are kept in accordance with the retention and disposal requirements set forth in reference (i).

(m) Ensure that any collection of information from individuals who are members of the public, as defined in reference (j), regardless of collection device used, has an approved and active OMB Control Number or has been officially determined to be exempt.

(n) Ensure records used in matching programs have an approved matching agreement in accordance with reference (a).

(o) Ensure that any contract for services where PII will be shared with or accessible to a contractor or its employees includes the Federal Acquisition Regulation (FAR), or Non-appropriated fund (NAF) equivalent, privacy clauses regarding the handling and safeguarding of PII. The applicable clauses are listed in reference (e).

(p) Ensure that individuals whose information is maintained in the system of records are able to review, obtain copies of, and correct any inaccurate information maintained in their records in accordance with the SORN.

4. Administration and Logistics

a. Records Management. Records created as a result of this Order shall be managed according to National Archives and Records Administration (NARA)-approved dispositions in reference (i), SECNAV M-5210.1 w/CH-1, to ensure proper maintenance, use, accessibility, and preservation, regardless of format or medium. Records disposition schedules are located on the Department of the Navy/Assistant for Administration (DON/AA), Directives and Records Management Division (DRMD) portal page at: https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/Records-and-Information-Management/Approved%20Record%20Schedules/Forms/AllItems.aspx. Refer to reference (l), MCO 5210.11F, for Marine Corps records management policy and procedures.

b. Privacy Act. Any misuse or unauthorized disclosure of Personally Identifiable Information (PII) may result in both civil and criminal penalties. The Department of the Navy (DON) recognizes that the privacy of an individual is a personal and fundamental right that shall be respected and protected. The DON's need to collect, use, maintain, or disseminate PII about individuals for purposes of discharging its statutory responsibilities shall be balanced against the individuals' right to be protected against unwarranted invasion of privacy. All collection, use, maintenance, or dissemination of PII shall be in accordance with the Privacy Act of 1974, as amended [reference (a)] and implemented per reference (b).

c. Forms. There are no forms used in this Order.

d. Records Dispositions

(1) This Order is assigned record schedule 5000-8.

(2) The records schedules used within this Order are: 5000-82.

e. Referenced/Related Websites

(1) USMC Privacy Act Website: https://www.hqmc.marines.mil/Agencies/USMC-FOIA/USMC-Privacy-Act/.

(2) USMC Privacy Program SharePoint Website: https://usmc.sharepoint-mil.us/sites/AR_HQMC_PA.

(3) DON CIO Privacy Website: https://www.doncio.navy.mil/TagResults.aspx?ID=36.

(4) DoD Privacy Website – System of Records Notices (SORNs): https://dpcld.defense.gov/Privacy/SORNsIndex/DOD-Component-Notices/.

(5) DoD CUI Program Website: https://www.dodcui.mil.

(6) Additional OMB Privacy Guidance Memoranda available at: https://www.fpc.gov/resources/omb/.

(7) Department of the Navy/Assistant for Administration (DON/AA), Directives and Records Management Division (DRMD) portal page: https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/Records-and-Information-Management/Approved%20Record%20Schedules/Forms/AllItems.aspx.

f. Updates. Updates made to this Order must be done in accordance with the current iteration of reference (ah).

g. Recommendations. Recommendations concerning the contents of this Order are welcomed and may be forwarded to the USMC Privacy Program Manager, AR (ARSF) via the appropriate chain of command.

5. Command and Signal

a. Command. This Order is applicable to the Marine Corps Total Force, to include all active duty and reserve military members, civilian and contractor employees, and non-appropriated funded employees.

b. Signal. This Order is effective the date signed.

G. P. OLSON
Director, Marine Corps Staff

DISTRIBUTION: PCN 10255306500

References

(a) 5 U.S.C. § 552a
(b) SECNAVINST 5211.5F
(c) DoDI 5400.11 w/CH-1, "DoD Privacy and Civil Liberties Programs," December 8, 2020
(d) DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
(e) DoDM 5400.11 Volume 2, "DoD Privacy and Civil Liberties Programs: Breach Preparedness and Response Plan," May 6, 2021
(f) SECNAV Memorandum, "Department of the Navy Breach Response Plan," February 12, 2019
(g) "New Department of the Navy Social Security Number (SSN) Reduction Plan," March 17, 2017
(h) DoDI 5400.16 w/CH-1, "DoD Privacy Impact Assessment (PIA) Guidance," August 11, 2017
(i) SECNAV M-5210.1 w/CH-1
(j) DoDM 8910.01 Volume 2 w/CH-3, "DoD Information Collections Manual: Procedures for DoD Public Information Collections," February 18, 2022
(k) DoDI 5200.48, "Controlled Unclassified Information (CUI)," March 6, 2020
(l) MCO 5210.11F
(m) MCO 5720.77
(n) Public Law 107-347, "E-Government Act of 2002," December 17, 2002
(o) Public Law 104-13, "Paperwork Reduction Act of 1995" May 22, 1995
(p) 10 U.S.C. § 130b, "Personnel in Overseas, Sensitive, or Routinely Deployable Units: Nondisclosure of Personally Identifying Information," 2011
(q) 42 U.S.C. § 2000ee-1, "Privacy and Civil Liberties Officers," 2010
(r) Executive Order 9397 (As Amended), "Numbering System for Federal Accounts Relating to Individual Persons," November 18, 2008
(s) 32 C.F.R. § 310, "Protection of Privacy and Access to and Amendment of Individual Records Under the Privacy Act of 1974," April 11, 2019
(t) OMB Circular No. A-108, "Federal Agency Responsibilities for Review, Reporting, and Publication Under the Privacy Act," December 23, 2016
(u) OMB Circular No. A-130, "Managing Information as a Strategic Resource" July 28, 2016
(v) M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002,"

September 26, 2003
(w) M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information," January 3, 2017
(x) M-18-02, "Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements," October 16, 2017
(y) DoDI 1000.30 w/CH-2, "Reduction of Social Security Number (SSN) Use Within DoD," November 30, 2022
(z) SECNAVINST 5720.42G
(aa) DoDI 8170.01 w/CH-1, "Online Information Management and Electronic Messaging," August 24, 2021
(ab) SECNAV M-5214.1
(ac) DoDI 6025.18, "Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoD Health Care Programs," March 13, 2019
(ad) DoDM 6025.18, "Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoD Health Care Programs," March 13, 2019
(ae) DoDM 8910.01 Volume 1 w/CH-4, "DoD Information Collections Manual: Procedures for DoD Internal Information Collections," December 5, 2022
(af) OSD Memorandum 17746-05, "Withholding of Information that Personally Identifies DoD Personnel," September 1, 2005
(ag) MCO 5216.9Y
(ah) MCO 5215.1K w/Admin CH-1

Headquarters Marine Corps (HQMC) Staff Offices/Commands and Subordinate Commands with Privacy Coordinators

The HQMC Staff Offices and commands listed below will designate a Privacy Coordinator. All other HQMC staff offices may designate a Privacy Coordinator or a Privacy POC based on need.

Headquarters Marine Corps (HQMC) Staff Offices	
Deputy Commandant for Information	DC I
Deputy Commandant for Manpower and Reserve Affairs	DC M&RA
Deputy Commandant for Plans, Policies, and Operations	DC PP&O
Staff Judge Advocate	JA
Major Subordinate Commands (MSCs)	
Marine Corps Installations Command	MCICOM
Marine Corps Logistics Command	MARCORLOGCOM
Marine Corps Recruiting Command	MCRC
Marine Corps Systems Command	MARCORSYSCOM
Marine Corps Forces Central Command	MARCENT
Marine Forces Command (Atlantic)	MARFORCOM
Marine Corps Forces Cyber Command	MARFORCYBERCOM
Marine Forces Europe and Africa	MARFOREURAF
Marine Corps Forces Korea	MARFORK
Marine Forces Northern Command	MARFORNORTHCOM
Marine Corps Forces Pacific	MARFORPAC
Marine Corps Forces Reserve	MARFORRES
Marine Corps Forces Southern Command	MARFORSOUTHCOM
Marine Forces Special Operations Command	MARSOC
Training and Education Command	TECOM
Subordinate Commands	
Marine Corps Installations Command East	MCIEAST
Marine Corps Installations Command West	MCIWEST
Marine Corps Installations Command Pacific	MCIPAC
Marine Corps Installations Command National Capital Region	MCINCR
I Marine Expeditionary Force	I MEF
II Marine Expeditionary Force	II MEF
III Marine Expeditionary Force	III MEF

Sample Privacy Coordinator Designation Letter (for Privacy Coordinator or Privacy Point of Contact (POC))

DEPARTMENT OF THE NAVY
U.S. MARINE CORPS ABC OFFICE / COMMAND
1234 MAIN STREET
CITY, ST 56789-0123

5211
(*Originator Code*)
(*Date*)

From: Commanding Officer, ABC Office / Command
To: Designated Individual

Subj: DESIGNATION AS PRIVACY COORDINATOR / PRIVACY POC

Ref: (a) 5 U.S.C. 552a
(b) SECNAVINST 5211.5F
(c) MCO 5211.5

1. In compliance with the provisions of references (a) through (c), you are designated as the (*Privacy Coordinator (major command level) / Privacy POC (subordinate command or unit level)*) for (*Command / Unit*). You will serve as the principal point of contact on PA matters and implement the provisions of references (a) through (c) and the Department of the Navy Privacy Program.

2. You are directed to familiarize yourself with the duties of the (*Privacy Coordinator / Privacy POC*), using references (a) through (c) and other directives as required in the performance of your duties.

3. Previous appointments as (*Privacy Coordinator / Privacy POC*) are revoked.

SIGNATURE
(*Commanding Officer/Acting*)

Copy to:
ARSF Privacy

APPENDIX A

Glossary of Acronyms and Abbreviations

AR	Administration and Resource Management Division
ARD	Publishing and Logistics Management Branch
ARDB	Records, Reports, Directives, and Forms Management Section
ARSF	Freedom of Information and Privacy Acts Office
ATSD-PCLT	Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency
BRT	Breach Response Team
CGIP	Commanding General's Inspection Program
CIO	Chief Information Officer
CMC	Commandant of the Marine Corps
CoRE	Critical or Required Evaluation
CUI	Controlled Unclassified Information
DC I	Deputy Commandant for Information
DoD	Department of Defense
DoDI	Department of Defense Instruction
DoDM	Department of Defense Manual
DON	Department of the Navy
DON CIO	Department of the Navy Chief Information Officer
DON/AA	Department of the Navy/Assistant for Administration
DRMD	Directives and Records Management Division
FAR	Federal Acquisition Regulation
FISMA	Federal Information Security Modernization Act
FOIA	Freedom of Information Act
HIPAA	Health Insurance Portability and Accountability Act
HQMC	Headquarters Marine Corps
IC4	Command, Control, Communications, and Computers Division
IG	Inspector General
IGMC	Inspector General of the Marine Corps
IT	Information Technology
MCO	Marine Corps Order
MSC	Major Subordinate Command
NAF	Non-appropriated Fund
NARA	National Archives and Records Administration
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PA	Privacy Act
PAS	Privacy Act Statement

PCLT	Privacy, Civil Liberties, and Transparency
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
POC	Point of Contact
SECNAV	Secretary of the Navy
SECNAVINST	Secretary of the Navy Instruction
SORN	System of Records Notice
SSN	Social Security Number
USMC	United States Marine Corps

APPENDIX B

Glossary of Terms and Definitions

1. Agency. For the purposes of disclosing records subject to the Privacy Act (reference (a)), the DoD is a considered a single agency. For all other purposes, to include requests for access and amendment, denial of access, or amendment, appeals from denials, and record keeping, as relating to the release of records to non-DoD Agencies, each DoD Component is considered an agency within the meaning of reference (a).

2. Headquarters Marine Corps (HQMC) Staff Office. Those offices identified in reference (ag) as staff offices.

3. Maintain/Maintenance. The collection, use, storage, dissemination and/or disclosure of records contained in a Privacy Act system of records.

4. Major Subordinate Command (MSC). Senior operational and supporting command. (Also listed in enclosure 2.)

5. Need to Know. A need for a record by an officer and/or employee of the agency which maintains the record in the performance of their official duties.

6. Privacy Act (PA) System Manager. An official responsible for overseeing the collection, maintenance, use, and dissemination of information from a PA system of records, regardless of format (paper or electronic). Systems managers are identified in the published SORNs.

7. Personally Identifiable Information (PII). Information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual, including but not limited to: name, date of birth, SSN (or any portion thereof), EDIPI/DoD ID number, biometrics, photograph, address, telephone number, e-mail address, mother’s maiden name, etc. Information that is not PII can become PII whenever additional information causes it to become linked or linkable to a specific individual.

Because there are many different types of information that can be used to distinguish or trace an individual’s identity, the term PII is necessarily broad. The DON recognizes two categories of PII, sensitive and non-sensitive. The sensitivity determines the level of protection necessary for maintaining the

information. Non-sensitive PII is still PII but may require less protection than sensitive PII.

NOTE: Non-sensitive information may become sensitive when aggregated or linked to other information.

8. Personally Identifiable Information (PII) Breach. A loss or suspected loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users have access or potential access (whether physical or electronic) to PII, and/or where PII is accessed for an unauthorized purpose.

9. Privacy Act (PA) System of Records. Any group of records where a record is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. (The key is that the record contains PII and is retrieved by PII.)

10. Privacy Coordinator. The individual designated by a HQMC staff office or USMC MSC to serve as the principal point of contact for Privacy Program matters for the staff office or MSC and subordinate commands/units in the chain of command. The Privacy Coordinator may also be referred to as the Privacy Act Coordinator or Privacy Official.

11. Privacy Impact Assessment (PIA). A written analysis to ensure PII in an IT system is collected, stored, protected, used, shared, and managed in a manner that protects privacy and conforms to applicable legal, regulatory, and policy requirements.

12. Privacy Point of Contact (POC). Individual designated to serve as the point of contact for Privacy Program matters for the subordinate command/unit.

13. Public-Facing Website. A website containing a collection of information which is freely accessible by all internet users, including members of the public.

14. Record. Any item, collection, or grouping of information, regardless of format (e.g., paper, electronic), about an individual that is maintained by a DoD Component.

15. Subordinate Command. All commands subordinate to a MSC.

16. System of Records Notice (SORN). A notice published in the Federal Register that constitutes official notification to the public of the existence of a System of Records. It informs the public of the purpose for the collection, what information may be maintained, about whom, who the information may be disclosed to on a routine basis, and the procedures for an individual to access their information and, if necessary, how to correct it.