DEPARTMENT OF THE NAVY
OFFICE OF THE SECRETARY
1000 NAVY PENTAGON
WASHINGTON DC 20350-1000

SECNAVINST 5211.5F
OCIO
20 MAY 2019

SECNAV INSTRUCTION 5211.5F

From: Secretary of the Navy

Subj: DEPARTMENT OF THE NAVY PRIVACY PROGRAM

Ref: See enclosure (1)

Encl: (1) References
(2) Definitions
(3) Responsibilities

1. Purpose

a. In accordance with the authority in reference (a), this instruction implements reference (b).

b. This issuance broadens the scope of the Privacy Act (PA) guidelines to include policy and procedures contained in reference (c), reference (d) and other associated privacy laws.

2. Cancellation. SECNAVINST 5211.5E.

3. Definitions. See enclosure (2).

4. Applicability

a. This instruction applies to the Offices of the Secretary of the Navy (SECNAV), the Chief of Naval Operations (CNO), the Commandant of the Marine Corps (CMC) and all United States Navy, United States Marine Corps installations, commands, activities, field offices, and all other organizational entities within the Department of the Navy (DON).

b. For the purposes of reference (a) and in accordance with Appendix II of reference (e), entities that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of (hereinafter, "maintain") information on behalf of the DON or that operate or use information systems on behalf of the DON, must comply with the privacy requirements in law, Office of

Management and Budget (OMB) policies, and Department of Defense (DoD) regulations.

5. Policy. It is DON policy that:

a. The privacy of an individual is a personal and fundamental right that will be respected and protected.

(1) The need to maintain personal information about individuals for purposes of discharging its statutory and regulatory responsibilities will be balanced against the right of the individual to be protected against unwarranted invasions of their privacy.

(2) The legal rights of individuals, as guaranteed by the Constitution, Federal law, regulations, and policies, will be protected when maintaining personal information about individuals.

(3) DON personnel have an affirmative responsibility to protect an individual's privacy when maintaining Personally Identifiable Information (PII) about an individual.

b. PII maintained by or for the DON will be:

(1) Relevant and necessary to accomplish a lawful DON purpose;

(2) Collected to the greatest extent practicable directly from the individual. The individual will be informed as to why the information is being collected, the authority for collection, what uses will be made of it, whether disclosure is mandatory or voluntary, and the consequences of not providing that information;

(3) Maintained only as authorized by this instruction and references (a), (b) and (f);

(4) Covered by an approved, published System of Records Notice (SORN) that permits such collection. SORNs will be approved and published in accordance with references (a), (b) and (g);

(5) Reviewed at least once a year to ensure the information is relevant, timely, complete, and accurate for its intended use;

(6) Protected from unauthorized access or disclosure; and

(7) Safeguarded with the appropriate administrative, technical, and physical controls, based on the media (paper, electronic, etc.) involved to ensure the security of the records and to prevent compromise or misuse during storage, transfer, or use, including when teleworking.

c. Use of Social Security Numbers (SSN) will be reduced or eliminated wherever possible in accordance with references (b), (f), and (h).

d. No record will be maintained on how an individual exercises rights guaranteed by the First Amendment to the Constitution, except as follows:

(1) When specifically authorized by statute;

(2) When expressly authorized by the individual about whom the record is maintained; or

(3) When the record is pertinent to and within the scope of an authorized law enforcement activity.

e. Individuals will be permitted, to the extent authorized by references (a), (b), and (f), to:

(1) Determine what records pertaining to them are contained in a system of records;

(2) Gain access to such records and obtain a copy of those records or a part thereof;

(3) Correct or amend such records once it has been determined that the records are not accurate, relevant, timely, or complete; and

(4) Appeal a denial of access or a request for amendment.

f. Disclosure of records pertaining to an individual from a system of records will be prohibited except with the consent of the individual or as otherwise authorized by references (a), (b), (f), and (i). When disclosures are made, the individual will be permitted, to the extent authorized by references (a), (b), and (f), to seek an accounting of such disclosures from the DON.

g. Disclosure of records pertaining to personnel assigned to overseas, sensitive, or routinely deployable units will be prohibited to the extent authorized by section 130b of reference (j).

h. DON personnel will conduct themselves consistent with the responsibilities described in enclosure (3).

i. When directed by the Senior Component Official for Privacy (SCOP), affected individuals will be notified in a timely manner if their PII, whether or not included in a system of records, is lost or suspected lost, stolen, or compromised.

j. DON Internet services and Internet-Based Capabilities used to maintain PII will be configured and operated in a manner that maximizes the protection (e.g., confidentiality, integrity, and availability) of the information commensurate with the risk of harm that could result from the loss, theft, or compromise of the PII, per reference (k).

k. Public-facing websites will be operated in compliance with the laws and requirements cited in reference (l).

l. Procedures to receive, investigate, respond to, and redress complaints from individuals who allege that the DON has violated their privacy can be found on the Department of the Navy Chief Information Officer (DON CIO) website.

6. Responsibilities. See enclosure (3).

7. Privacy Act. Any misuse or unauthorized disclosure of PII may result in both civil and criminal penalties. All collection, use, maintenance, or dissemination of PII will be in accordance with the Privacy Act of 1974, as amended (reference (a)) and this document.

8. Records Management

a. Records created as a result of this instruction, regardless of format or media, must be maintained and dispositioned according to the records disposition schedules found on the Directives and Records Management Division (DRMD) portal page: https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/SitePages/Home.aspx.

b. For questions concerning the management of records related to this instruction or records disposition schedules, contact your local Records Manager or the DRMD program office.

9. Forms and Reports

a. Forms. SECNAV 5211/1 (Rev. 5/2019), DON Loss or Compromise of PII Breach Reporting Form and SECNAV 5211/2 (Rev. 5/2019), DON Loss or Compromise of PII After Action Report, and SECNAV 5213/1 (Rev. 5/2019), SSN Reduction Review are available at Naval Forms Online at: https://www.secnav.navy.mil/doni/default.aspx.

b. Reports. The reporting requirements contained in enclosure (3) are assigned the following SECNAV Report Control Symbols: SECNAV 5211-1, DON Loss or Compromise of PII Breach Reporting Form; SECNAV 5211-2, DON Loss or Compromise of PII After Action Report; SECNAV 5213-1, SSN Reduction Review, per reference (n).

THOMAS B. MODLY
Under Secretary of the Navy

Distribution:
Electronic only, via Department of the Navy Issuances website https://www.secnav.navy.mil/doni.

REFERENCES

(a) 5 U.S.C. §552a
(b) DoD Directive 5400.11 of 29 October 2014
(c) Public Law 107-347
(d) Public Law 104-13
(e) OMB Circular No. A-130 of 28 July 2016
(f) DoD 5400.11-R of 14 May 2007
(g) OMB Circular No. A-108 of 23 December 2016
(h) DoD Instruction 1000.30 of 1 August 2012
(i) SECNAVINST 5720.42F
(j) 10 U.S.C. §130b
(k) DoD Instruction 8550.01 of 11 September 2012
(l) SECNAVINST 5720.44C
(m) DoD Instruction 5400.16 of 11 August 2017
(n) SECNAV M-5214.1

DEFINITIONS

1. Access. The ability or opportunity to gain knowledge of PII.

2. Accountable Command. Normally this term is used to identify the command responsible for causing a PII breach and for completing actions to mitigate the risk of harm to affected individuals.

3. Amendment. The process of adding, deleting, or changing information in a system of records to make the data accurate, relevant, timely, or complete.

4. Confidentiality. An expressed and recorded promise to withhold the identity of a source or the information provided by a source.

5. Disclosure. The transfer of any PII from a system of records by any means of communication (such as oral, written, electronic, mechanical, or actual review) to any person, private entity, or Government Agency, other than the subject of the record, the subject's designated agent, or the subject's legal guardian.

6. DON Personnel. Officers and employees of the DON, members of the uniformed Services (including members of the Reserve Components), and individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the United States (including survivor benefits). For purposes of reference (a), DON personnel include contractors under a current DON contract.

7. Individual. Under the Privacy Act, a citizen of the United States or an alien lawfully admitted for permanent residence. The custodial parent of a minor or the legal guardian of any individual also may act on behalf of an individual. Members of the United States Armed Forces are "individuals". Corporations, partnerships, sole proprietorships, professional groups, businesses, whether incorporated or unincorporated, and other commercial entities are not "individuals".

8. Information Systems. A discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information.

9. Maintain. Term used throughout this instruction to describe PII that is created, collected, used, processed, stored, disseminated, disclosed, or disposed of PII.

10. Official Need to Know. Within the context of this instruction, this term is used when DON officials and employees have a demonstrated need for the use of any record or the information contained therein in the performance of their official duties.

11. Privacy Impact Assessment (PIA). A written analysis of how information is handled to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, and determines the risks and effects of maintaining PII in an information technology (IT) system registered in Department of Defense Information Technology Portfolio Registry-DON (DITPR-DON). It also examines and evaluates protections and alternative processes for handling information to mitigate potential privacy risks.

12. PII. Per reference (e) the term PII refers to 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. 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. To determine whether information is PII, the agency will perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available -in any medium or from any source -that would make it possible to identify an individual. The DON recognizes two categories of PII, sensitive and non-sensitive. Non-sensitive information may become sensitive when aggregated or linked to other information.

13. PII Breach. A suspected or actual loss of control, compromise, unauthorized disclosure, unauthorized acquisition,

unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to PII, whether physical or electronic.

14. Privacy Coordinator. For purposes of this instruction the individual within their command designated to manage the organization's privacy program. The Privacy coordinator is also known as the Privacy Act Coordinator or Privacy Official.

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

16. Record. Any item, collection, or grouping of information, whatever the storage media (e.g., paper, electronic), about an individual that is maintained by a DoD Component. Information may include, but is not limited to an individual's education, financial transactions, medical history, criminal or employment history, and that contains his or her name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print, or a photograph.

RESPONSIBILITIES

1. DON CIO has authority for privacy policy and oversight of the DON Privacy Program for all DON commands and activities.

2. Director, Office of the Chief Information Officer

a. Serves as the DON SCOP;

b. Develops and implements DON privacy policy;

c. Serves as the principal advisor on all DON privacy matters;

d. Oversees the administration of the DON privacy program;

e. Oversees DON privacy online website;

f. Develops and oversees a DON-wide privacy training program;

g. Integrates protection of PII into the information system life cycle management process per reference (c);

h. Provides guidance for effective assessment and use of privacy-related technologies;

i. Serves as the DON PIA review and approval official;

j. Ensures that all DON Secretariat, Navy and Marine Corps programs or systems that maintain PII on members of the public, DON personnel, contractors (based on applicable contract requirements) or foreign nationals employed at U.S. military facilities overseas, have a PIA completed in accordance with reference (m) and approved by the DON SCOP prior to the collection of PII;

k. Posts the summaries of all approved PIAs to the DON CIO website;

l. Ensures that no information is collected and maintained in a DON system of records without the existence of an approved, published SORN that permits such collection. SORNs will be

approved and published in accordance with references (a), (b), and (g);

m. Represents the DON at meetings called by the DoD Privacy, Civil Liberties, and Transparency Division (DPCLTD);

n. Represents the DON on the DoD Data Integrity Board;

o. Represents the DON at DoD Senior Agency Official for Privacy meetings;

p. Establishes DON PII breach reporting procedures;

q. Reviews all breach reports for the DON and after completing a risk assessment, determines if affected personnel should receive written notification of a PII breach. This responsibility may be delegated to respective Navy and Marine Corps privacy offices;

r. Determines when commands responsible for a breach are to provide identity protection services; and

s. Consolidates input received for the annual Federal Information Security Management Act (FISMA) privacy report and submits the approved report to the DPCLTD.

3. U.S. Navy Office of Information

a. Develops and administers Navy and Marine Corps website privacy policies and procedures respectively per reference (k);

b. Maintains master world wide web page to provide new service-specific web privacy guidance;

c. Maintains overall cognizance for DON websites and website content-related questions as they pertain to website privacy requirements;

d. Ensures that public-facing websites have machine-readable privacy policies; and

e. Provides input to the DON SCOP for inclusion in the annual FISMA report submission to DoD.

4. CNO. The Office of the CNO is responsible for the administration and supervision of the actions and activities required by this instruction within the Navy. To ensure Navy implementation of information privacy protections, including full compliance with federal laws, regulations, and policies relating to information privacy, the Office of the CNO will appoint personnel, delegate authorities and direct development and issuance of Service guidance, as required, to execute this instruction within the Navy.

a. Ensures Navy PA compliance efforts are coordinated Service-wide;

b. Ensures Navy personnel and contractors (based on applicable contract requirements) receive appropriate training regarding privacy laws, regulations, and policies governing DoD-specific procedures for handling of PII. The mandatory DON annual privacy computer based training course meets these requirements;

c. Ensures there is a Navy privacy instruction that defines program requirements and responsibilities within the Navy including PII breach reporting procedures;

d. Ensures appropriate Navy representation at DPCLTD meetings;

e. Ensures that all Navy systems and applications that maintain PII about members of the public, DON personnel, contractors (based on applicable contract requirements) or foreign nationals employed at U.S. military facilities overseas, have a PIA completed in accordance with reference (m) and approved by the DON SCOP prior to the collection of PII;

f. Maintains a Navy privacy website and related content;

g. Conducts annual staff assistance visits/program evaluations of at least one Navy Echelon II command to review compliance with all privacy laws, DoD Guidance, and this

instruction. The DON SCOP should be made aware of any significant findings requiring corrective action;

h. Compiles and submits reports as required to the DON SCOP (e.g., FISMA);

i. Implements the DON SSN reduction plan in accordance with DoD and DON policy;

j. Ensures PA systems of records are kept in accordance with retention and disposal requirements set forth in reference (n);

k. Ensures protection of PII is integrated into the information system life cycle management process for all Navy IT systems, per reference (c);

l. Ensures a privacy coordinator is designated at all Navy Echelon II and III Commands to serve as a principal point of contact on privacy matters;

m. Ensures SORNs are reviewed annually to ensure they are necessary, accurate, up-to-date, and appropriately scoped, and advise the applicable Privacy Office (Navy or Marine Corps) promptly of the need to establish, modify, or delete a SORN;

n. Ensures no official files are maintained on individuals that are retrieved by name or other personal identifier without first ensuring that a SORN exists that permits such collection;

o. Ensures PII breaches are reported and follow-up actions are conducted including individual notifications and/or remediation;

p. Ensures self-inspections are conducted using the PII Compliance Checklist found on the DON CIO website at least twice annually; and

q. Ensures PA complaints are processed, investigated, and resolved.

5. CMC. The Office of the CMC is responsible for the administration and supervision of the actions and activities required by this instruction within the Marine Corps. To ensure

Marine Corps implementation of information privacy protections, including full compliance with federal laws, regulations, and policies relating to information privacy, the Office of the CMC will appoint personnel, delegate authorities and direct development and issuance of Service guidance, as required, to execute this instruction within the Marine Corps.

a. Ensures Marine Corps PA compliance efforts are coordinated Service-wide;

b. Ensures Marine Corps personnel and contractors (based on applicable contract requirements) receive appropriate training regarding privacy laws, regulations, and policies governing DoD-specific procedures for handling of PII. The mandatory DON annual privacy computer-based training course meets these requirements;

c. Ensures there is a Marine Corps Marine Corps Order that defines program requirements and responsibilities within the Marine Corps, including PII breach reporting procedures;

d. Ensures appropriate Marine Corps representation at DPCLTD meetings;

e. Ensures that all Marine Corps systems and applications that maintain PII about members of the public, DON personnel, contractors (based on applicable contract requirements) or foreign nationals employed at U.S. military facilities overseas, have a PIA completed in accordance with reference (m) and approved by the DON SCOP prior to the collection of PII;

f. Maintains a Marine Corps privacy website and related content;

g. Conducts annual staff assistance visits/program evaluations of at least one Marine Corps major command to review compliance with all privacy laws, DoD Guidance, and this instruction. The DON SCOP should be made aware of any significant findings requiring corrective action;

h. Compiles and submits reports as required to the DON SCOP (e.g., FISMA);

i. Implements the DON SSN reduction plan in accordance with DoD and DON policy;

j. Ensures PA systems of records are kept in accordance with retention and disposal requirements set forth in reference (n);

k. Ensures protection of PII is integrated into the information system life cycle management process for all Marine Corps IT systems per reference (c);

l. Ensures a privacy coordinator is designated at all Marine Corps major and sub commands to serve as a principal point of contact on privacy matters;

m. Ensures SORNs are reviewed annually to ensure they are necessary, accurate, up-to-date, and appropriately scoped, and advise the applicable Privacy Office (Navy or Marine Corps) promptly of the need to establish, modify, or delete a SORN;

n. Ensures no official files are maintained on individuals that are retrieved by name or other personal identifier without first ensuring that a SORN exists that permits such collection;

o. Ensures PII breaches are reported and follow-up actions are conducted including individual notifications and/or remediation;

p. Ensures self-inspections are conducted using the PII Compliance Checklist found on the DON CIO website at least twice annually; and

q. Ensures PA complaints are processed, investigated, and resolved.

7. DON Personnel. Personnel that use or maintain PII on behalf of the DON will:

a. Comply with DoD and DON privacy policy to ensure PII is protected and the confidentiality, integrity, and availability of the information is preserved;

b. Complete privacy training, as required. The mandatory DON annual privacy training course meets this requirement. Navy

Service Member privacy training requirements are defined annually via a NAVADMIN;

c. Not disclose PII, by any means of communication, to any person or other entity, except as authorized by this instruction or the specific SORN;

d. Properly mark all documents containing PII (e.g., letters, emails, message traffic, etc.,) as "FOR OFFICIAL USE ONLY - PRIVACY SENSITIVE - Any misuse or unauthorized disclosure can result in both civil and criminal penalties;"

e. Upon discovery, report any unauthorized disclosure of PII to the applicable Privacy coordinator or supervisor;

f. Report unauthorized collections of PII to the applicable Privacy coordinator or supervisor;

g. Not store DON PII, other than his/her own PII, on any personal electronic storage device, including laptops, tablets, and cell phones/smart phones; and

h. Ensure all records are kept in accordance with retention and disposal requirements set forth in reference (n).

8. DON Contracting Officials. In addition to complying with duties and responsibilities listed in paragraph 7 of this enclosure, contracting officials will:

a. Ensure contracts comply with Federal Acquisition Regulation and Defense Federal Acquisition Regulation privacy provisions;

b. Ensure the design, development, or operation of a system of records or maintaining PII is only to accomplish a DON function or mission, subject to references (b), (f), and the following:

(1) Contractor-owned or maintained IT systems under contract to DON must be registered in the DITPR DON.

(2) Unauthorized disclosure of PII by DON contractor personnel (based on applicable contract requirements) through negligence or misconduct can lead to contractor removal or,

depending on the severity of the disclosure, contract termination.

(3) Contractors (based on applicable contract requirements) responsible for the unauthorized disclosure of PII, may be held accountable for any costs associated with breach mitigation, including those incurred as a result of having to notify personnel.

c. Ensure contractors (based on applicable contract requirements) sign a non-disclosure agreement as a condition of contractor access to PII;

d. Ensure upon discovery of a PII breach or suspected breach, will immediately notify their DON chain-of-command or Contracting Officer Representative (COR); and

e. Ensure upon discovery of unauthorized collections of PII, contractor personnel (based on applicable contract requirements) will immediately notify their DON chain-of-command or COR.

9. Foreign Nationals employed at U.S. military facilities overseas. When collecting PII on foreign nationals employed on United States military facilities overseas, the applicable data protection authority and/or local written agreements for each country applies.

10. Program Managers. Program managers are responsible for overseeing the collection, maintenance, use, and dissemination of information from a system of records and ensuring that all personnel who have access to those records are aware of their responsibilities for protecting PII that is being maintained in the system of records. In this capacity, they will:

a. Establish appropriate administrative, technical, and physical safeguards to ensure the records in the system of records for which they are responsible are protected from unauthorized alternation, destruction, or disclosure;

b. Protect the records from reasonably anticipated threats or hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained;

c. In coordination with their Privacy Coordinator, annually review each SORN under their cognizance to determine if the records are up-to-date and/or used in matching programs and whether they are in compliance with OMB guidelines. Such items as organization names, titles, addresses, etc., frequently change and should be updated;

d. Work with the command Privacy Coordinator to complete a PIA and SORN as required for all new and existing systems that maintain PII;

e. Stop collecting any PII that is no longer justified, and, when feasible, remove the information from existing records;

f. Ensure all records are kept in accordance with retention and disposal requirements set forth in reference (n);