DEPARTMENT OF THE NAVY
BUREAU OF NAVAL PERSONNEL
5720 INTEGRITY DRIVE
MILLINGTON, TN 38055-0000

BUPERSINST 5211.7A
BUPERS-07
24 Aug 2018

BUPERS INSTRUCTION 5211.7A

From: Chief of Naval Personnel

Subj: BUREAU OF NAVAL PERSONNEL PRIVACY PROGRAM AND ESTABLISHMENT OF THE BUREAU OF NAVAL PERSONNEL PRIVACY CADRE

Encl: (1) References
(2) Definitions

1. Purpose

a. This instruction formally establishes the Bureau of Naval Personnel (BUPERS) Privacy Program and the BUPERS Privacy Cadre.

b. The primary purpose of this instruction is to describe privacy policies prescribed by the BUPERS Privacy Program regarding the proper handling of personally identifiable information (PII) and protected health information (PHI) for all employees who require access to such information in the performance of their official duties or who are charged with ensuring sensitive PII and PHI are handled per law, Executive Order, or policy. BUPERS employees must comply with all agency policies and procedures and manage per guidance contained in references (a) through (af), contained in enclosure (1).

c. This instruction formally establishes the BUPERS privacy cadre, which is a key component of the BUPERS Privacy Program. The primary purpose of the privacy cadre is to develop and maintain a core group of privacy trained professionals available to facilitate the proper handling of sensitive PII and PHI by continuously increasing the overall privacy consciousness of the organization and to ensure compliance with mandated spot checks and PII training. The privacy program consists of voluntary members.

d. Major revisions to this instruction include clarification of BUPERS guidance for protecting PII, inclusion of policy for data transfers, and update of references applicable to PII protection. It also includes two new policies: completion of Department of the Navy (DON)

Annual Privacy Training prior to being granted access to Navy-Marine Corps Intranet (NMCI), and the requirement for all employees to sign a statement of understanding acknowledging their responsibility to protect and safeguard PII. This instruction is a complete revision and should be read in its entirety.

2. Cancellation. BUPERSINST 5211.7.

3. Scope and Applicability. This instruction applies to all military personnel, civilian employees, and contract and sub-contract employees in BUPERS Millington, Navy Personnel Command (NAVPERSCOM), Navy Recruiting Command (NAVCRUITCOM), Navy Manpower Analysis Center (NAVMAC), Navy consolidated brigs and their subordinate commands and detachments, and personnel support detachments (PSD). This instruction also applies to foreign nationals who are employed within BUPERS/NAVPERSCOM, NAVCRUITCOM, NAVMAC, and subordinate commands.

4. Discussion. Privacy is a civil liberty that, by law, each individual is entitled to per reference (a). In our business, Sailors, Marines, and civilians routinely entrust BUPERS with their PII and PHI, and it is BUPERS responsibility to ensure the systems and processes we employ safeguard this sensitive information. Protecting personnel privacy must be taken very seriously and all measures must be considered and implemented to protect their PII. Members of the BUPERS enterprise have access to a significant amount of sensitive PII and every member who has access to PII and PHI is responsible for safeguarding and protecting it per all laws, policy, and guidance to prevent unauthorized access, dissemination and or destruction, and accessing PII and PHI for business reasons only. In support of the BUPERS Privacy Program and privacy cadre, applicable references and definitions are contained in enclosures (1) and (2).

5. Action. Due to the large volume of PII and PHI collected, maintained, accessed, used, transported, disclosed, and destroyed throughout the BUPERS enterprise, all personnel who have access to PII and PHI must:

a. Be properly trained to not only comply with law but also to ensure sensitive information (controlled unclassified information) does not fall into the hands of those who would seek to cause harm. Our processes rely heavily on PII and PHI; therefore, extra attention and care must be taken to ensure all personnel know how to identify, mark, and handle sensitive PII and PHI. It is everyone's responsibility to prevent a breach, and should a breach occur, required steps must be taken to ensure reporting and processing per references (b) and (c):

(1) Personnel who have discovered a known or suspected loss of PII or unauthorized access to PII must report the breach and all suspected breaches to their supervisor per reference (c), who will contact the BUPERS Privacy Program manager.

(2) PSD staff will contact the PII coordinator in NAVPERSCOM Pay and Personnel Management Department (PERS-2) to report the actual or potential loss of PII. The PERS-2 PII coordinator will work with the BUPERS Privacy Program manager to determine if the breach is 'high risk,' which would necessitate a formal breach report to be submitted. If a breach report is required, it will be submitted by the PSD that mishandled the PII.

(3) Personnel who 'mishandle' PII must take the PII refresher training, which is available on the Department of the Navy (DON) Chief Information Officer Web site. This includes military, civilian, and contract and sub-contractor employees.

(4) Personnel must also report all known security incidents so they can be adjudicated and proper actions taken if it is determined that the incident involves PII or PHI.

b. Be able to identify and safeguard sensitive PII and PHI and be familiar with the requirements for marking and handling this material as outlined in reference (d), especially when this information is being e-mailed.

c. Digitally sign, encrypt, and properly label all e-mails containing information for official use only and e-mails containing unclassified, sensitive information per references (d) and (e). The subject line of an e-mail containing PII must be labeled "FOUO_PRIVACY SENSITIVE…". Social security numbers (SSN) (full or truncated) are forbidden in the subject line, as the subject line is never encrypted. Names are allowed in the subject line as long as there is no other identifying information (medical diagnosis, disciplinary action, etc.). The body of the e-mail containing PII must contain the privacy warning: "FOR OFFICIAL USE ONLY – PRIVACY SENSITIVE. Any misuse or unauthorized disclosure may result in both civil and criminal penalties."

d. Not mail or send by courier sensitive PII on CDs, DVDs, hard drives, flash drives, floppy disks, or other removable media unless the data is encrypted and properly packaged. If mailing PII using United States Postal Service (USPS), Federal Express (FedEx), United Parcel Service (UPS), etc., it must be sent in packaging containing Tyvek.

e. Confine the use of records containing PII and PHI to that information required in the performance of official duties (need to know). Be cognizant of data aggregation and how it can increase the sensitivity of the information and severity of a potential breach.

f. Protect information under reference (a), the Privacy Act (PA), and never willfully disclose information to an individual or agency not authorized access to such information. Not all PII is subject to reference (a), but all PII must be protected.

g. Never access, ask for, obtain, share, or receive personal data under false pretenses, or when there is no business need to know or if the PII or PHI is not required for an official use per reference (f). Unacceptable uses of PII will not be tolerated. Periodic audits to identify such access to PII may be conducted and investigated if necessary. The following situations are examples of inappropriate access to PII and are violations of reference (a) and must be reported as high risk breaches:

(1) Out of curiosity

(2) As a favor for a co-worker

(3) After high-visibility incidents, and

(4) Without a business need to know

h. Ensure customers are informed of the risks of providing sensitive and non-sensitive information to BUPERS commands and activities via unsecure means. Some business processes require employees to solicit sensitive information from customers who do not have the means to send the information encrypted. In these situations, employees must ensure customers are made aware of the risk of sending PII unencrypted and provide them with alternate methods of transmission. These alternate methods include:

(1) U.S. Army Aviation and Missile Research Development Center, Safe Access File Exchange (SAFE). If using SAFE it is highly recommended that documents containing PII are password-protected prior to being uploaded to SAFE.

(2) Letter, using the USPS

(3) Unencrypted e-mail, only after specific circumstances (e.g., non-common access card (CAC) holder). BUPERS employees must consult with and be granted approval from the BUPERS Privacy Program Manager when soliciting PII.

(4) Fax, use properly labeled cover sheet and ensure the recipient is available to retrieve the transmission immediately.

i. Ensure they provide a PA advisory to an individual any time they collect the SSN, or portion thereof, from an individual and this information is not going to be retained in a system of record per reference (d);

j. Ensure they provide a Privacy Act statement (PAS) to an individual any time they collect PII (name, SSN, etc.) from an individual and this data could possibly be retained in a system of record per reference (d).

k. Ensure all electronic and paper documents (letters, reports, spreadsheets, etc.) containing PII are properly labeled with the privacy warning "FOR OFFICIAL USE ONLY – PRIVACY SENSITIVE. Any misuse or unauthorized disclosure may result in both civil and criminal penalties." The naming convention for files that contain PII must begin with 'FOUO_Privacy Sensitive' and should never contain the SSN (full or truncated).

l. Use DD 2923 Privacy Act Data Cover Sheet to protect PII. This form should be used on folders containing PII, when mailing PII (paper and CD), when transporting PII, when faxing, and to protect PII on a desk. The DD 2923 should not be considered a replacement method for protecting PII on a desk when a more secure means should be used (placing documents in a drawer, etc.). This form must not be posted on file cabinets, desk drawers, or any container that contains PII because it simply draws attention to where the PII can be found.

m. Secure PII in a desk drawer or file cabinet when not in use and when walking away from their desk (regardless of the length of time the owner may be away), where it could be compromised or when leaving for the day. PII must not be left on desks unattended. Although allowed, red bins containing PII must be kept out of plain sight at all times and, if at all possible, the PII must be disposed of at a frequency that prevents the bin from overflowing. PII must be destroyed such that it is rendered unrecognizable and cannot be reconstructed.

n. Fax only as a last resort. Per references (h) and (i), ensure the fax number has been provided by the recipient, verified before faxing, use the DD 2923, and request the recipient to acknowledge receipt of the document(s).

o. Not remove PII from the workplace except as authorized by reference (j). When transporting PII or when teleworking, documents removed from government workspaces must be properly secured in envelopes or folders with a DD 2923 affixed to the front. The envelope will be double-wrapped with the DD 2923 affixed to the inner package. The employees' supervisor must approve, with a memorandum for the record, the removal of all PII from the workspace.

Telework agreements must indicate the employee is authorized to remove paper PII from the workplace. Documents must be secured at the alternate work location in a manner consistent with this instruction and must not be transported to or used in a public area (e.g., library, coffee shop, etc.). When removing PII from the workspace that is stored on Department of Defense (DoD)-owned equipment, the device must:

(1) Be signed in and out with a supervising official who has been designated in writing by the department head 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) Be enabled to encrypt all PII stored, created, or written from laptop computers and removable storage media, as applicable.

p. Must not store any PII on personally-owned laptop computers, mobile computing devices, and removable storage media. Documents containing PII maintained on network (shared) drives should only be accessible by those with a need-to-know and should be properly marked per references (k), (l), and (m).

q. Must properly dispose of PII when it is no longer relevant or required per references (d) and (f). 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). PII should never be placed in a recycling bin unless it has been shredded with a cross-cut shredder and destroyed so as not to be reconstructed. Electronic storage media and information systems containing PII must be disposed of per reference (n). Reference (a) requires agencies to review current holdings of PII and ensure they are accurate, relevant, timely, and complete; reduce PII holdings to the minimum necessary for proper performance of agency functions; develop a schedule for periodic review of PII holdings; and establish a plan to eliminate the unnecessary collection and use of SSNs. The use of strip shredders is strictly forbidden.

r. Owners of business processes involving sensitive PII and PHI must ensure mechanisms are in place to protect this information and ensure their employees are trained on their responsibility for protecting PII and PHI. Personnel must not be asked to provide sensitive information using an unsecure means or when there is not a need to know. Business units must not use a group or code e-mail address to facilitate business processes involving sensitive

information unless e-mail encryption is possible. Group mailboxes that capture PII are allowed, provided they have a soft certificate (i.e., the credentials required to encrypt or read encrypted e-mail in a group mailbox) prior to receiving any sensitive information;

s. To prevent the risk of PII or PHI data compromise, all requests for data are to be submitted through the compliance review process, which is an administrative safeguard observed to ensure records in each system of record are protected from unauthorized access, alteration, or disclosure and that their confidentiality is preserved and protected. The data compliance review process is managed and administered by the Enterprise Information Management (EIM) team, which is located in BUPERS Command Information Office (BUPERS-07). Per BUPERSINST 5239.4 (Data Transfer), the transfer of data from an information technology (IT) application or system to any other application, system, office, or person is not authorized until the EIM team has vetted the data request and has obtained approval for the transfer. The only exceptions to this policy are congressional inquiries, which are addressed by BUPERS Office of Legal Counsel (BUPERS-00J); and Freedom of Information Act (FOIA) requests which are addressed by the BUPERS Privacy Act Officer.

t. System owners must ensure all system of records notices (SORN) are published in the Federal Register, per reference (a). They are also responsible for ensuring their respective SORNs are reviewed per reference (o) when there are significant changes to the system. Significant changes include, but are not limited to:

(1) a substantial increase in the number, type, or category of individuals about who records are maintained in the system;

(2) a change that expands the types of categories of records maintained in the system;

(3) a change that modifies the scope of the system;

(4) a change that modifies the purpose(s) for which the information in the system of records is maintained;

(5) a change in the agency's authority to maintain the system of records or maintain, collect, use, or disseminate the records;

(6) a change that modifies the way in which the system operates or modifies its location;

(7) a change to equipment configuration (either hardware or software); and

(8) a new routine use or significant change to an existing routine use

u. System owners who are responsible for the operation of a system of records (to include pilot programs) are responsible for ensuring a privacy impact assessment (PIA) is completed for each of their systems and applications (information systems) as early in the development process as possible per references (p) and (q). PIAs are risk assessments designed to identify the risks and associated mitigations of collecting and maintaining PII. They are to be updated every 3 years or when significant changes are made to the IT asset.

v. System owners will be responsible for ensuring privacy- by-design (PbD) is, to the greatest extent possible, implemented from the beginning of the life-cycle management process.

w. Review business processes that collect or use the SSN to determine the feasibility of either removing the SSN or replacing it with an alternate unique identifier such as the DoD-identification number (DoD-ID). References (r), (s), (t), and (u) prescribe the requirements to reduce the use of the SSN in IT systems, business processes, and miscellaneous documents (e.g., Excel spreadsheets, reports, and lists, etc.). Additional requirements include:

(1) All new and modified policies that require the collection or use of the SSN must either attempt to replace the SSN with the DoD-ID or justify the continued use of the SSN using SECNAV 5213/1 SSN Justification Memo.

(2) All information systems that collect or maintain the SSN must either remove the SSN or replace it with the DoD-ID. Those information systems that must continue utilizing the SSN must have a SECNAV 5213/1 completed and signed by the BUPERS Command Information Officer (CIO) (BUPERS-07).

(3) SSNs must 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 (r). Every effort should be made to explore whether SSNs can be substituted with the DoD-ID when possible. The disclosure of the last four numbers of the SSN to individuals without a need to know constitutes a PII breach that must be reported per reference (b). All documents that contain the SSN must be labeled with the privacy warning “FOR OFFICIAL USE ONLY – PRIVACY SENSITIVE. Any misuse or unauthorized disclosure may result in civil and criminal penalties”.

(4) Any time an SSN is used in a briefing slide, user manual, or standard operating procedure, etc., the fictitious SSN, 000-00-000, will be used instead of an actual SSN. If the last four of the SSN is required, it will be ‘0000’. In situations where the SSN is embedded in a screen-shot, it must be either removed or permanently redacted.

(5) Never use SSNs in personnel rosters, surveys, or questionnaires or post them on a public-facing Web site.

(6) Electronic folder and or file names must not contain the SSN.

(7) SSNs are prohibited in the subject line of e-mails, naval messages, letters, or memorandums per reference (u).

x. Ensure privacy training is completed annually for all employees, to include military, civilian, contractors and subcontractors when the contract requires access to PII. No more than 1 year should elapse between training, per references (v) and (w). Annual training is authorized to be taken online or in classroom settings. Employees must complete DON Annual Privacy training and Cyber-Awareness training prior to being granted access to NMCI.

y. Generally, those breaches that are clearly the result of human error will not require an investigation. Breaches that are determined to be caused by willful neglect or with malicious intent will be investigated. Any breach determined to have been caused by willful neglect or with malicious or criminal intent will be reviewed by BUPERS Security Manager (BUPERS-00Y). The type of investigation to be conducted will be determined by Deputy Chief of Naval Personnel (BUPERS-00B) with recommendation from BUPERS-00J; BUPERS Director, Human Resources and Manpower (BUPERS-05) (if civilians are implicated in the incident). Military members are subject to reference (ac), civilians are subject to reference (ad), and contractor incidents will be handled by the appropriate contracting officer's representative. Be aware of the potential disciplinary and administrative actions that may be levied on those who negligently or willfully violate privacy-related laws and policies (references (ab), (ac), and (ad)).

z. Ensure that, consistent with reference (x), clauses 52.204-21, Basic Safeguarding of Contractor Information Systems; 52.224-1 Privacy Act Notification; 52.224-2 Privacy Act; and 52.224-3 Privacy Training; are included in contracts for the operation of a system of records and or all work that requires handling of Federal information. PII is allowed on vendor devices only after receiving approval from the contracting officer's representative and the applicable Federal Acquisition Regulation clauses are included in the applicable contract. All contract personnel working on behalf of the Navy must comply with the Navy's PII training requirement. Ensure contractors have been informed of their responsibilities regarding the Department of the Navy (DON) PA Program and ensure they understand what is considered PII and comply with all BUPERS protocols and policy for handling it.

aa. Always maintain control of the CAC. This means the CAC must be removed from the CAC reader each and every time employees leave their computer workstation. The CAC must not be shared with other employees or left unattended in a workspace, regardless of the security of the room or building.

bb. All employees (military, civilian, contractors and sub-contractors) will read and sign the BUPERS Employee PII Handling Statement of Understanding NAVPERS 5211/16. New employees must sign the NAVPERS 5211/6 prior to being granted access to NMCI.

6. Privacy Cadre. The BUPERS Privacy Cadre was established to comply with reference (d) and is comprised of the BUPERS Privacy Program Manager and the Privacy Cadre;

a. The BUPERS Privacy Program manager will act as the lead for the privacy cadre and will be the liaison between BUPERS and NAVPERSCOM and external commands (DON Privacy Office, etc.). Responsibilities for the Privacy Program manager are listed in the designation letter.

b. The Privacy Cadre will be comprised of PII coordinators from throughout the BUPERS organization to include NAVMAC, NAVCRUITCOM, brigs, and PSDs. They will comply with responsibilities listed in their designation letters.

(1) For BUPERS Millington and NAVPERSCOM, the PII coordinator and subordinate code PII coordinators will be designated in writing by Deputy Chief of Naval Personnel (BUPERS-00B).

(2) For NAVCRUITCOM, the command PII coordinator will be designated by Commander, Navy Recruiting Command.

(3) Commanding Officer, NAVMAC will sign designation letters for PII coordinators assigned to NAVMAC.

(4) Commanding officers of Navy brigs will sign the designation letters for PII coordinators assigned to the brigs' staff.

(5) Officers in charge and directors of PSDs will sign designation letters for their PII coordinators.

c. Members of the Privacy Cadre are charged with assuming an active leadership role in their sphere of influence in the effort to protect sensitive PII and PHI. Any person (military or civilian) with a professional or personal interest in protecting personal information may seek membership in the privacy cadre.

7. Records Management. Records created as a result of this instruction, regardless of media and format, must be managed per reference (y).

8. Review and Effective Date. Per OPNAVINST 5215.17A, BUPERS-07 will review this instruction annually on the anniversary of its issuance date to ensure applicability, currency, and consistency with Federal, DoD, Secretary of the Navy (SECNAV), and Navy policy and statutory authority using OPNAV 5215/40 Review of Instruction. This instruction will be in effect for 5 years, unless revised or cancelled in the interim, and will be reissued by the 5-year anniversary date if it is still required, unless it meets one of the exceptions in OPNAVINST 5215.17A, paragraph 9. Otherwise, if the instruction is no longer required, it will be processed for cancellation as soon as the cancellation is known, following the guidance in OPNAV Manual 5215.1 of May 2016.

9. Forms

a. The following DoD forms are available for download via the DoD Forms Program Management Web site, http://www.dtic.mil/whs/directives/forms/dd/ddforms2500-2999.htm:

(1) DD 2923 Privacy Act Data Cover Sheet

(2) DD 2930 Privacy Impact Assessment (use to prepare and submit PIAs)

b. SECNAV Forms

(1) The following SECNAV forms are available for download via Naval Forms Online, https://navalforms.documentservices.dla.mil/web/public/home

(a) SECNAV 5211/1 Department of the Navy Loss or Compromise of Personally Identifiable Information (use to submit a PII breach report)

(b) SECNAV 5211/2 Department of the Navy Loss or Compromise of Personally Identifiable Information After Action Reporting (use to submit an after action report).

(2) SECNAV 5213/1 SSN Justification Memo (use to justify the continued use of the SSN in an IT system or business process) is available for download at http://www.public.navy.mil/bupers-npc/reference/forms/NAVPERS/Pages/default.aspx

c. The following NAVPERS forms are available for download at http://www.public.navy.mil/bupers-npc/reference/forms/NAVPERS/Pages/default.aspx

(1) NAVPERS 5211/15 PII Assessment Checklist (use to conduct mandated PII assessments and spotchecks)

(2) NAVPERS 5211/16 Employee PII Handling Statement of Understanding (use to ensure employee acknowledgment of their responsibilities to properly handle and protect PII)

J. W. HUGHES
Deputy Chief of Naval Personnel

Distribution and releasability:
This instruction is cleared for public release and is available electronically only via BUPERS/NAVPERSCOM Web site, http://www.public.navy.mil/bupers-npc/Pages/default.aspx

REFERENCES

References are archived on and are available on the BUPERS Privacy Cadre Web page at https://mpte.navy.deps.mil/sites/organizations/Privacy/PrivacyCadre/SitePages/Home.aspx .

Ref: (a) 5 U.S.C. §552A
(b) DON CIO 291652Z Feb 08
(c) OMB memo M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information of 3 Jan 2017
(d) SECNAVINST 5211.5E
(e) DON CIO 032009Z Oct 08
(f) DoD 5400.11-R, DoD Privacy Program, May 2007
(g) DON CIO 151450Z Mar 17
(h) DON CIO 171625Z Feb 12
(i) DON CIO 081745Z Nov 12
(j) DoD Instruction 1035.01 of 4 April 2012
(k) DON CIO 281759Z Aug 12
(l) DON CIO 201839Z Nov 08
(m) DON CIO 171952Z Apr 07
(n) DON CIO 281759Z Aug 12
(o) OMB memo Circular No. A-108, Federal Agency Responsibilities for Review, Reporting, and Publication Under the Privacy Act of 23 Dec 2016
(p) 44 U.S.C. § 208 Ch.36
(q) DoD Instruction 5400.16 of 14 July 2015
(r) DoD Instruction 1000.30 of 1 August 2012
(s) DON CIO 192101Z Jul 10
(t) DON CIO 171625Z Feb 12
(u) DON CIO 151450Z Mar 17
(v) DON CIO 181905Z Feb 08
(w) SECNAV WASHINGTON DC 231552Z Jan 97 (ALNAV 07/07)
(x) FAR clauses 52.224-1, 5224-2, 52.224-3, and 52.204-21,
(y) SECNAV M-5210.1 of January 2012
(z) SECNAV WASHINGTON DC 251830Z Mar 16 (ALNAV 019/16)
(aa) SECNAV WASHINGTON DC 232026Z Jul 07 (ALNAV 057/07)
(ab) SECNAV WASHINGTON DC 051800Z Jan 16 (ALNAV 01/16)
(ac) UCMJ
(ad) SECNAVINST 12752.1A
(ae) OMB memo M-07-16, Subj: Safeguarding Against and Responding to the Breach of PII of 22 May 2007
(af) DoD 6025.18-R, DoD Health Information Privacy Regulation, January 2003

DEFINITIONS

Access. The ability or opportunity to gain knowledge of personally identifiable information (PII) or a record contained in a system of records by an individual.

Agency. For the purposes of disclosing records subject to the Privacy Act (PA) between or among Department of Defense (DoD) components, DoD is 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, Department of the Navy (DON) is considered an agency within the meaning of the PA.

Alteration. A significant modification of a system of records notice (SORN) involving the increase or change in the number or type of individuals about whom records are maintained; increases that expand the types of categories of records; a significant change in the purpose for maintaining the records; a change in the "authority for maintenance of the system; an additional or new means of indexing and retrieving records; the addition of a routine use; or an addition of or change to an exemption.

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

Breach. The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII information for an other than authorized purpose. A breach may include the loss or theft of physical documents that include PII and portable electronic storage media that store PII, the inadvertent disclosure of PII or a public Web site, or an oral disclosure of PII to a person who is not authorized to receive that information.

Contractor. Any individual or other legal entity that: Directly or indirectly (e.g., through an affiliate) submits offers for or is awarded, or reasonably may be expected to submit offers for or be awarded a government contract, including a contract for carriage under government or commercial bills of lading, or a subcontract under a government contract; or conducts business, or reasonably may be expected to conduct business, with the Federal Government as an agent or representative of another contractor.

Controlled Unclassified Information. Unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and Government-wide policies.

Data Aggregation. Any collection in which information is gathered and expressed in a summary form, such as statistical analysis. A common aggregation purpose is to compile information about particular groups based on specific variables such as age, profession, or income. Data aggregation increases the severity of a breach if the data is compromised.

Department of Defense – Identification Number (DoD-ID). A unique 10-digit number that is associated with personnel and their common access card (CAC). The DoD-ID is assigned to each person registered in the Defense Enrollment and Eligibility Reporting System (DEERS). This includes government civilians, active duty military, dependents, reservists, retirees, and contractors. In time, the DoD-ID number will replace the social security number (SSN) in many DON and DoD business processes. The DoD-ID and name are only considered sensitive PII when additional information is added to the name and DoD-ID combination.

Disclosure. The information sharing or 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, government agency, or private entity, other than the subject of the record, the subject's designated agent, or the subject's legal guardian.

For Official Use Only (FOUO): A record designation, not a classification.

Foreign National Employee. An individual who is employed by or performing work for the DON outside the United States, its territories, and possessions. For the purpose of a privacy impact assessment (PIA) only, foreign national employees are considered DON employees.

Harm to an Individual. Includes any negative or unwanted effects (i.e., that may be socially, physically, or financially damaging) to an individual. Examples of harm to individuals include, but are not limited to, identity theft, physical harm, discrimination, the potential for blackmail, the disclosure of private facts, mental pain and emotional distress, financial harm, the disclosure of contact information for victims of abuse, the potential for secondary uses of the information which could result in fear or uncertainty, or the unwarranted exposure leading to humiliation or loss of self-esteem.

Incident. An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

Individual. A living person who is 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 may also act on behalf of an individual. Members of the Military Services are individuals. Corporations, partnerships, sole proprietorships, professional groups, businesses, whether incorporated or unincorporated, and other commercial entities are not individuals when acting in an entrepreneurial capacity with the DoD, but are individuals when acting in a personal capacity (e.g., security clearances or entitlement to DoD privileges or benefits).

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

Life-cycle Management (LCM). Also referred to as Total Life Cycle System Management. LCM is the implementation, management, and oversight by the program manager of all activities associated with the acquisition, development, production, fielding, sustaining, and disposal of a DON information technology (IT) system.

Maintain. The term is used to describe the collection, maintenance, use, or dissemination of PII or records contained in a system of records.

Make PII Available. Any DON action that causes PII to become available or accessible to the DON, whether or not the DON solicits or collects it. An individual can make PII available to the DON when he or she provides, submits, communicates, links, posts, or associates PII while using the Web site or application. "Associate" can include activities commonly referred to as "friending," "following," "liking," joining a "group," becoming a "fan," and comparable functions.

Mixed System of Records. Any system of records that contains information about individuals as defined by the PA and non-U.S. citizens and or aliens not lawfully admitted for permanent residence.

Need to Know. A determination that an individual requires access to specific information in the performance of (or assist in the performance of) lawful and authorized government functions and duties. It is a preventative measure to identify and deter unauthorized access. When determining 'need to know', rank, and position are insignificant.

Non-Sensitive (Roladex) Personal Identifiable Information (PII). Non-sensitive PII is PII, which if lost, compromised, or disclosed without authorization would not result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. A number of these elements are used for internal government operations and are releasable under the Freedom of Information Act. Examples are work phone number and work e-mail address. PII is defined in reference (aa).

Official Need to Know. A determination that a prospective recipient requires access to, use, or need knowledge of specific information in order to perform or assist in a lawful and authorized governmental function.

Official Use. 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.

Operation of a System of Records. To perform any of the activities associated with maintaining a system of records, including the collection, use, transportation, and dissemination of records.

Personally Identifiable Information (PII). Information used to distinguish or trace an individual's identity, such as name, SSN, date and place of birth, mother's maiden name, biometric records, home phone number, and other demographic, personnel, medical, and financial information. PII includes any information that is linkable to a specified individual, alone, or when combined with other personal or identifying information. The term PII also includes personal information and information in identifiable form. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-sensitive PII can become sensitive PII whenever additional information is made publically available – in any medium and from any source – that, when combined with other available information, could be used to identify an individual.

PII Breach. This term is used to include the 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. A breach is not limited to a network intrusion, targeted attack that exploits Web site vulnerabilities, or an attack executed via e-mail or attachment. A breach may include the loss or theft of physical documents and portable electronic storage media, or an oral disclosure of PII to a person who is not authorized to receive that information.

- Willful Breach of PII. When an individual deliberately or intentionally disregards DON security or privacy safeguarding policies or requirements (e.g., intentionally provides sensitive PII to individuals who do not have an official need to know), causing harm to an individual.

- (PII Breach caused as a result of) Willful Neglect. When an individual's reckless indifference for DON security or privacy safeguarding policies or requirements results in a breach of PII which causes harm to an individual.

PII Coordinator. Individual appointed by a department to serve as the principal point of contact (POC) on PII matters, including breach reporting, training, and mandatory spot checks.

Privacy Act Advisory. A statement provided to an individual when the individual is requested to provide his or her SSN, or a portion thereof, for identification purposes and the SSN will NOT be retained in a system of records. The statement informs the individual of the authority and purpose for the collection of the information and whether providing the information is mandatory or voluntary.

Privacy Act Statement (PAS). A statement provided to an individual when the individual is requested to provide PII (name, date of birth, SSN, etc.) for possible inclusion in a system of records. The statement informs the individual of the authority and purpose for the collection of the information, the routine uses for which the information may be disclosed, and whether providing the information is mandatory or voluntary. The statement enables the individual to make an informed decision whether to provide the information requested. A PAS must include all the elements found in reference (e), section C2.1.4.2.

Privacy-by-Design (PbD). An approach to system engineering which takes privacy into account throughout the entire engineering process.

Privacy Cadre. A core group of privacy trained professionals, consisting of voluntary members, that facilitate the proper handling of sensitive PA and PII material by applying expertise and continuously increasing the overall privacy consciousness in the organization. Each member of the cadre is formally designated.

Privacy Impact Assessment (PIA). An analysis of how information is handled: (1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (2) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system, and (3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. It is an ongoing assessment for IT systems to evaluate adequate practices and balance privacy concerns with the security needs of an organization. The process is designed to guide owners and developers of information systems in assessing privacy through the early stages of development.

Privacy Program Manager. Individual appointed by a command to serve as the principal POC on privacy (PII) matters.

Privacy Warning. A statement used on documents (both paper and electronic) containing PII, e-mails and faxes with attachments containing PII, and systems or containers which hold files or records containing PII to notify personnel of the nature of the contents so that proper handling and access controls can be maintained.

Protected Health Information (PHI). A subset of PII. Per reference (ab), PHI is individually identifiable health information that is transmitted or maintained by electronic or any other form or medium, except as otherwise contained in employment records held by a covered entity in its role as an employer. In addition to the protections and requirements required under the PA and other privacy laws, PHI is subject to the Health Information Portability and Accountability Act.

Record. Any item, collection, or grouping of information, regardless of storage media (e.g., paper, electronic, etc.), about an individual that is maintained by a DON activity that contains the individual's name or other identifying particulars assigned to the individual.

Records Management. The planning, controlling, directing, organizing, training, promoting, and other managerial activities related to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the U.S. Government and effective and economical management of agency operations. Within the DON, records management is implemented by reference (u).

Risk Assessment. An analysis considering information sensitivity, vulnerabilities, and cost in safeguarding PII processed or stored in the facility or activity.

Routine Use. A disclosure of a record made outside DoD for a use that is compatible with the purpose for which the record was collected and maintained by DoD and which is included in the published SORN for the system of records involved.

Sensitive PII. Sensitive PII is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Sensitive PII requires stricter handling guidelines because of the increased risk to an individual if the data is compromised. Some categories of PII are sensitive as stand-alone data elements, including SSNs or biometric identifiers. Other data elements such as a financial account number, citizenship status, or medical information, in conjunction with the identity of an individual (directly or indirectly inferred), is also considered sensitive PII. In addition, the context of the PII may determine whether the PII is sensitive, such as a list of employees with poor performance ratings.

Spillage. Incidents involving the unauthorized disclosure of classified material.

System Owner. An official who has overall responsibility for a system of records.

System of Records. A group of records under the control of a DON component from which PII is retrieved by the individual's name or by some identifying number, symbol, or other identifying particular uniquely assigned to an individual. PII that is extracted from a system of record, exported to a spreadsheet or report, and subsequently used to retrieve individual information by a unique identifier is considered to be an 'extension' of the system of record. The original SORN for the system of record must include this extraction in the routine uses portion of the SORN.

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.