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 (ab).

   c. This instruction also serves to formally establish 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.

2. Cancellation. BUPERSINST 5211.6 and BUPERSINST 5230.9.
3. **Scope and Applicability.** This instruction applies to all military personnel, civilian employees, and contract employees in BUPERS Millington, Navy Personnel Command (NAVPERSCOM), Navy Recruiting Command (NAVCRUITCOM), Navy Manpower Analysis Center (NAVMAC), Navy consolidated briggs and their various subordinate commands and detachments, and personnel support detachments (PSD) and customer service desks (CSD). 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 us with their PII and PHI and it is our responsibility to ensure the systems and processes we employ safeguard this sensitive information. Protecting the privacy of our personnel must be taken very seriously and all measures must be considered and implemented in order to protect their PII. Members of the BUPERS enterprise have access to a significant amount of PII and every member who has access to PII is responsible for safeguarding and protecting it per all laws, policy, and guidance to prevent unauthorized access, maintenance, dissemination and or destruction, and accessing PII 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 reference (b):

      (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, who will contact the BUPERS Privacy Program manager.

      (2) Personnel stationed at a PSD or CSD will contact the PII coordinator in NAVPERSCOM, Pay and Personnel Management Department (PERS-2) to report the actual or potential loss of PII.
(3) Personnel who ‘mishandle’ PII must take the PII refresher training.

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

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 (c), especially when being emailed;

c. Digitally sign, encrypt, and properly label all e-mails containing official business and e-mails containing unclassified, sensitive information per reference (d);

d. Not mail or courier sensitive PII on CDs, DVDs, hard drives, flash drives, floppy disks, or other removable media unless the data is encrypted and properly packaged;

e. Confine their use of records containing PII and PHI to their area of responsibility and only access that information required in the performance of their official duties. Be cognizant of data aggregation and how it can increase the 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 do so, or if the PII or PHI is not required for an official use per reference (e). Unacceptable uses of PII will not be tolerated without consequences. 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 do so

h. Ensure customers are informed of the risks of providing sensitive and non-sensitive information to BUPERS/NAVPERSCOM 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)

(2) Letter, using the U.S. Postal Service

(3) Unencrypted email

(4) Fax

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

   j. Ensure they provide a Privacy Act (PA) 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 (c);

   k. Ensure all electronic and paper documents (records) containing PII is 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 should begin with ‘FOUO_Privacy Sensitive’, and if the file is being emailed, the privacy warning must be included in the body of the email;

   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, and to protect PII on a desk. 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 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 (f) and (g), ensure the fax number has been provided by the recipient, use 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 (h). 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 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). 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 (i), (j), and (k).

q. Must properly dispose PII when it is no longer relevant or required per references (c) and (e). 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. Electronic storage media and information systems containing PII must be disposed of per reference (l). 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. ‘Strip’ shredders are 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 email address to facilitate business processes involving sensitive information unless email encryption is possible;

s. 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 every 2 years and the applicable amendment, alteration, or cancellation is submitted. System of records may also include mixed system of records;

t. System owners who are responsible for the operation of a system of records (to include pilots) 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 (m) and (n). 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;

u. System owners are responsible for ensuring privacy by design is, to the greatest extent possible, implemented from the very beginning of the life-cycle management process;

v. 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 (o), (p), and (q) prescribe the requirement to reduce the use of the SSN in information technology (IT) systems, business processes, and miscellaneous documents (Excel spreadsheets, reports, and lists, etc.). Additional requirements include:

(1) All new and modified policies that require the collection or use of the SSN and either attempt to replace the SSN with the DoD ID or justify the continued use of the SSN.

(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 an SSN justification memo 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 (o).
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).

(4) Any time an SSN is used in a brief, user manual, or standard operating procedure, etc., the fictitious SSN, 000-00-000, will be used instead of a live, real 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 permanently redacted.

(5) Never use SSNs in personnel rosters or post them on a public-facing Web site;

(6) Electronic folder and or file names will not contain the SSN;

w. Ensure privacy training is completed annually for all employees, to include military, civilian, and contractors and no more than 1 year should elapse between training, per references (r) and (s).

x. 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. The type of investigation to be conducted will be determined by BUPERS, Office of Legal Counsel (BUPERS-00J). Military members are subject to reference (y), civilians are subject to reference (z), 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 (x), (y), and (z)).

y. Ensure, consistent with reference (t), subparts 24.1, 52.224-2, 39.105, 39.106, 52.239-1, and 4.19 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;

z. Always maintain control of their common access card (CAC). This means it must be removed from the CAC reader each and every time employees leave their desk. It must not be shared with other employees or left unattended in a workspace, regardless of the security of the room or building.
6. **Privacy Cadre.** The BUPERS privacy cadre was established to comply with reference (c) 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 the brigs, PSDs, and CSDs. They will comply with responsibilities listed in their designation letters;

      (1) For BUPERS Millington/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.

   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 material. 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 (u).

8. **Review and Effective Date.** Per OPNAVINST 5215.17A, BUPERS-07 will review this instruction annually on the anniversary of its effective 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. OPNAV 5215/40 may be obtained from BUPERS, Directives Manager (BUPERS-01). This instruction will automatically
expire 5 years after effective date unless reissued or cancelled prior to the 5-year anniversary date, or an extension has been granted.

9. Forms

a. DD 2923 Privacy Act Data Cover Sheet is available for download via the DoD Forms Program Management Web site, http://www.dtic.mil/whs/directives/forms/dd/ddforms2500-2999.htm

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

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

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

c. Use NAVPERS 5211/15 PII Assessment Checklist to conduct mandated PII assessments and spot checks. NAVPERS 5211/15 is available for download at http://www.public.navy.mil/bupers-npc/reference/forms/NAVPERS/Pages/default.aspx

R. A. BROWN
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

Ref:  
(a) 5 U.S.C. §552A
(b) DON CIO 291652Z Feb 08
(c) SECNAVINST 5211.5E
(d) DON CIO 032009Z Oct 08
(e) DoD 5400.11-R, Department of Defense Privacy Program, May 2007
(f) DON CIO 171625Z Feb 12
(g) DON CIO 081745Z Nov 12
(h) DoD Instruction 1035.01 of 4 April 2012
(i) DON CIO 281759Z Aug 12
(j) DON CIO 201839Z Nov 08
(k) DON CIO 171952Z Apr 07
(l) DON CIO 281759Z Aug 12
(m) 44 U.S.C. § 208 Ch.36
(n) DoD Instruction 5400.16 of 14 July 2015
(o) DoD Instruction 1000.30 of 1 August 2012
(p) DON CIO 192101Z Jul 10
(q) DON CIO 171625Z Feb 12
(r) DON CIO 181905Z Oct 08
(s) SECNAV WASHINGTON DC 231552Z Jan 97 (ALNAV 07/07)
(t) FAR, Subparts 24.1 and 24.2, 52.224-1 and 52.224-2, 39.105, 39.106, 52.239-1, 4.19
(u) SECNAV M-5210.1
(v) SECNAV WASHINGTON DC 251830Z Mar 16 (ALNAV 019/16)
(w) SECNAV WASHINGTON DC 232026Z Jul 07 (ALNAV 057/07)
(x) SECNAV WASHINGTON DC 051800Z Jan 16 (ALNAV 01/16)
(y) UCMJ
(z) SECNAVINST 12752.1A
(aa) OMB memo M-07-16, Subj: Safeguarding Against and Responding to the Breach of PII of 22 May 2007
(ab) DoD 6025.18-R, DoD Health Information Privacy Regulation, January 2003
DEFGINITIONS

**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.

**Amendment.** The minor modification of a system of records notice (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.

**Alteration.** A significant modification of a 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.

**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 and for an other than authorized purpose have access or potential access to PII, whether physical or electronic.

**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 Department of the Navy (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.

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.

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

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.

Non-Sensitive 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. 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.

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

**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).** PbD is the architecting of things with privacy in mind from the very beginning of the lifecycle.

**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 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 defined as 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 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), are 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 Manager.** 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.

**Willful PII Breach (willful neglect).** When an individual purposefully 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 the individual. Harm includes embarrassment, inconvenience, financial loss, blackmail, identity theft, emotional distress, and loss of self-esteem.