Frequently Asked Questions - General Information

01. What is the Privacy Act?

The Privacy Act of 1974 is a code of fair information practices which mandates how Government agencies, such as OSD, shall maintain records about individuals. The Privacy Act requires that Government agencies: collect only information that is relevant and necessary to carry out an agency function; maintain no secret records on individuals; explain at the time the information is being collected, why it is needed and how it will be used; ensure that the records are used only for the reasons given, or seek the person's permission when another purpose for their use is considered necessary or desirable; provide adequate safeguards to protect the records from unauthorized access and disclosure; allow people to see the records kept on them and provide them with the opportunity to correct inaccuracies in their records.

02. Does the Privacy Act apply to all Government records?

No. The Privacy Act only applies to Government records that: contain information on individuals; are maintained by a Government agency or its contractors in a system of records; and are retrieved by a personal identifier, such as a person's name, Social Security Number, medical record number or other unique identifier.

03. Does the Privacy Act apply to all records maintained about individuals?

No. The Privacy Act only applies to U.S. citizens or lawful permanent resident aliens and only to Government records that meet the requirements outlined in item 2 above. The Privacy Act does not apply to deceased persons.

04. What is a System of Records?

A system of records (SOR) is a group of records under the control of a Federal government agency from which personal information about an individual is retrieved by the name of the individual, or by some other identifying number, symbol, or other unique identifier.

05. What is a System of Records Notice (SORN)?

A system of records notice (SORN) is a description of any Privacy Act system of records. SORNs generally describe the 'who, what, where, and why' of a system and describe the processes for individuals to access or contest the information being held on them in that system. SORNs are required to be published in the Federal Register for a public comment period before the system data collection (paper based or electronic) can be started.

06. Does the OSD/JS have any Privacy Act Systems of Records?

Yes. The OSD/JS Privacy Act systems of records may be found at the following site: http://dpcld.defense.gov/Privacy/SORNs.aspx.

07. How does the Government inform the public about the record systems that are covered by the Privacy Act?

The Government informs the public about record systems covered by the Privacy Act by publishing notices in the Federal Register. The record systems are referred to as Privacy Act systems of records and the notices provide a description of particular systems of records.

08. What are an individual's basic rights and the agency employees' responsibilities under the Privacy Act?

The following is a summary of an individual's rights and the OSD/JS employee responsibilities under the Privacy Act regarding:

A. Collection of Personal Information

Individual Rights: As an individual, whenever you are requested to provide personal information to a Federal agency, you are entitled to know the following: the legal authority for requesting the information, the purpose for collecting it, what related uses might be made of this information, whether your response is mandatory or voluntary, and what effect your refusal to provide the information would have.

Employee Responsibilities: As an employee, you must collect only personal information that is relevant and necessary to accomplish an authorized agency function. Whenever you request personal information from someone, you must inform him/her in writing of the legal authority, the purpose for collecting it, what related uses will be made of this information, whether a response is mandatory or voluntary, and what will be the effect if he/she refuses to respond. This information usually is provided on a form given to the person providing the information. Whenever you ask for a Social Security Number you must tell the individual the purpose for requesting it, and whether a response is mandatory or voluntary. You should always attempt to collect personal information directly from the individual rather than from other sources.

B. Access to Records

Individual Rights: As an individual, you can request to see your records in writing or in person. You should describe the information you wish to see because blanket requests for "all the information the agency has on me" cannot be honored. If you appear in person, identification will be required to verify you are the person whose record you are requesting. If you have no suitable identification, you will be asked to certify your identity in writing. Telephone requests are usually not honored, because positive identification of the caller may be difficult to establish. You may have another person accompany you when you review your records. You are entitled to receive a copy of your record or an acknowledgement of your request within ten working days. You are not required to give a reason for your request; however, the more specific your request, the faster you can expect a response.

Employee Responsibilities: As an employee, when someone requests to see his or her record, you must verify his/her identity or require written certification that he or she is the subject of the record requested.

If a patient requests another person's presence when he/she wants to inspect or discuss his/her records, you must have the patient authorize the other person's presence in writing prior to the inspection or discussion of the records.

When a request for a record is received, you should check to see whether a record exists on the person in a system of records that is subject to the Privacy Act. Depending on the procedure in your organization, the system manager or designee must either present the record or a copy of it, or acknowledge the request within ten working days.

You should not ask the person to give a reason or justify a need to see his or her own record.

C. Access to Health and Medical Records

Individual Rights: Special rules apply to health and medical records. As an individual, you should usually be able to see your medical record directly. However, when it appears that the medical record may contain information that could have an "adverse effect" on you, the medical record will be sent to a representative you name, such as your family doctor or other responsible person, who would be willing to review the medical record and inform you of its contents. You may designate an OSD/JS employee as your representative.

Employee Responsibilities: As an employee, when an individual requests access to their own medical record, you must require that they designate a representative, such as a family doctor or other health professional or other responsible person, who would be willing to review the record and discuss its contents. The responsible official may determine that the medical record will not have an "adverse effect" upon the person and allow direct access to the medical record. A patient may designate an OSD/JS employee as his/her representative. As with all records subject to the Privacy Act, the individual's identity must be verified.

D. Amendment of Records
Individual Rights: As an individual, if you wish to correct, delete or add information, you must identify the record and give your reasons for the desired change. In general, only factual, verifiable information is subject to amendment under the Privacy Act. Other procedures, such as personnel grievance procedures, should be followed if you wish to contest subjective opinion. You must verify your identity as described above. Employee Responsibilities: As an employee, depending on your organization's procedures, you or a designated official must acknowledge a request to amend a record within ten working days and advise the person when he or she can expect a decision on the request. A review should normally be completed within 30 days. You must verify the person's identity. Advise the person when he or she can expect a decision on the request. Under the regulations, an appeal must be decided within 30 days which may be extended an additional 30 days.

09. What can I do to meet my Privacy Act responsibilities?

If the Privacy Act is to achieve its objectives, there must be cooperation by every employee and contractor who works with records containing individually identifiable information. In the course of your work you become a steward of the information entrusted to you. In order to meet the responsibilities of this stewardship, there are certain steps you should to take: a. Learn the requirements of the Privacy Act and how they relate to your particular job. This can be accomplished through formal training, on-the-job training, discussions with your supervisor, and reading. Acquaint yourself as much as possible with the Privacy Act policies and procedures that apply to the information that you work with day-to-day. b. Consider how you handle the information you work with, and what measures, if any, you need to take to safeguard the personal information that you have about others in your possession. c. Certain OSD staff are specially trained in the requirements of this law and they are available to assist you. Your supervisor can give the name of your nearest Privacy Act official. d. Respond promptly to requests for information by quickly referring such requests to the responsible OSD/JS Privacy Act official. Learn the procedures used for Privacy Act requests and follow them when requests for information are received. e. Be careful that personal information is not disclosed to anyone unless that individual has received prior permission to see the information from the subject of the record, or disclosures of the record are authorized by law. The Privacy Act authorizes disclosure of an OSD/JS Privacy Act record to OSD/JS employees who have a legitimate need for the record in the performance of their duties.

10. Does the Privacy Act apply to all OSD/JS employees?

Yes. As an OSD/JS employee you "wear two hats." On the one hand you are an individual citizen who is entitled to the full protection and rights afforded by the Privacy Act. On the other hand, you are a Federal employee who works with records containing personal information and who shares some responsibility in carrying out the requirements of the law. Unless you are a Privacy Act system manager or designee, you should never disclose information subject to the Privacy Act from the records in your care or allow unauthorized persons access to such records. The seriousness of this responsibility is evident from the penalties the Privacy Act imposes for knowing and willful violations of the law. Fines up to $5,000 can be imposed by the courts for willfully disclosing personal information that should not be released under the Privacy Act. Disciplinary actions may include reprimand, suspension, or termination of employment.

11. Does the Privacy Act apply to contractors?

Yes, whenever a contractor establishes or maintains a system of records to carry out a function of OSD; the following clauses should be inserted in the solicitations and contracts: 52.224-1, Privacy Act Notification and 52.224-2, Privacy Act.

12. What does it mean to make a routine use disclosure from a Privacy Act System of Records?

A routine use disclosure from a Privacy Act system of records permits disclosures of information from a record to requestors outside OSD without the consent of the individual to whom the record pertains. Routine use

disclosures must be consistent with the purpose(s) for which the information was collected and must be published in the Federal Register. Routine use disclosures are not mandatory. They are optional disclosures made at the discretion of the appropriate Privacy Act System Manager or his/her designee. Agencies must keep an accounting of all disclosures made pursuant to a routine use.

13. What is "Personally Identifiable Information (PII)"?

Information used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, biometric records, home phone numbers, other demographic, personnel, medical, and financial information. PII includes any information that is linked or linkable to a specified individual, alone, or when combined with other personal or identifying information.

14. What is Identity Theft?

Identity theft is a rapidly growing crime that exploits your personal information in order to open false accounts in your name, or to access your current accounts fraudulently. Identity thieves can accrue thousands of dollars of debt in your name and leave you and your family to foot the bill. Additionally, identity theft can leave your credit record in shambles, making it harder to qualify for loans, and possibly jobs, in the future. Identity thieves can commit crimes in your name, leaving you with a criminal record.
Most identity theft begins with seemingly innocent events. A stolen wallet or checkbook can easily turn into a stolen identity, and missing personnel records can give thieves a gold mine in personal information. Identity theft can come from many sources.

Stealing mail, checks, or personnel records.
Dumpster Diving: Rummaging through trash for bills or other personal documents.
Changing Your Address: Using change of address processes, thieves can divert mail, including bank statements, credit card statements, and credit offers in order to access your information and accounts.
Phishing: A popular method of information theft, phishing entails sending fraudulent emails claiming to be from financial institutions or companies needing your personal information. Phishing can include redirecting you to official looking 'dummy' websites that gather your information, under the pretext of reputable financial institutions - often your own bank or credit company.
Skimming: At stores or restaurants that you frequent, your personal and credit card information could be in jeopardy. Identity thieves can use technologically advanced card readers to collect your information from credit cards which they process for your everyday purchases. Wait staff or clerks can scan your card when you make purchases and save the information for later manipulation.

15. What should I do if I suspect my identity has been stolen?

Mitigating the harm of identity theft can be a complicated process, and time can be of the essence. For information on specific steps to be taken in response to identity theft, see the Federal Trade Commission's website at http://www.consumer.ftc.gov/features/feature-0014-identity-theft.

16. What are Privacy Impact Assessments (PIAs) and where can I find them?

A PIA is needed on DoD Information Technology (IT) and electronic collections that collect, maintain, use, or disseminate PII to:

Ensure Personally Identifiable Information (PII) handling conforms to applicable legal, regulatory, and policy requirements regarding privacy.
Determine the need, privacy risks, and effects of collecting, maintaining, using, and disseminating PII in electronic form.
Examine and evaluate protections and alternative processes to mitigate potential privacy risks.

Performed when PII about members of the public (i.e., DoD personnel, contractors, or foreign nationals employed at U.S. military facilities internationally), is collected, maintained, used, or disseminated in electronic form.
Performed on DoD IT and electronic collections including those supported through contracts with external sources that collect, maintain, use, or disseminate PII about members of the public, DoD personnel, contractors, or in some cases foreign nationals.
The DoD PIAs are located on the DoD CIO Website.
Additional guidance can be found in the DoD Instruction 5400.16
A PIA is completed using the DD Form 2930, "Privacy Impact Assessment (PIA)."