



Defense Privacy, Civil Liberties,

and Transparency Division

U.S. Department of Defense

Search DPCLD: -

- [Home](#)
- [Privacy](#)
 - [About the Office](#)
 - [SORNs](#)
 - [Privacy Contacts](#)
 - [Resources](#)
 - [Privacy Act Request](#)
 - [Authorities and Guidance](#)
 - [Matching Agreements](#)
 - [Privacy Impact Assessments](#)
- [Civil Liberties](#)
 - [About the Office](#)
 - [Resources](#)
 - [Authorities and Guidance](#)
- [Media](#)
- [Reports](#)
- [Department of Defense](#)
- [Contact](#)

PRIVACY

[About the Office](#)

[Authorities & Guidance](#)

[ID Theft Resources](#)

[Privacy POCs](#)

FREQUENTLY ANSWERED QUESTIONS

Below are some questions commonly asked of the DoD Privacy Office.

- [What is personally identifiable information \(PII\)?](#)
 - [What are examples of personally identifiable information \(PII\)?](#)
 - [What are the risks if personally identifiable information \(PII\) is misused?](#)
 - [Why should I be interested in the Privacy Act?](#)
 - [What information is covered under the Privacy Act?](#)
 - [What is a System of Records?](#)
 - [What is a System of Records Notice \(SORN\)?](#)
 - [How does the government inform the public about personally identifiable information \(PII\) being held in its records systems that are covered by the Privacy Act?](#)
 - [Who can I contact if I have additional questions about the privacy of my information?](#)
 - [What does it mean when a system of record notice refers to a routine use?](#)
 - [How will I know if an incident has possibly occurred that resulted in a significant compromise of my personally identifiable information \(PII\)?](#)
 - [What do I do if I receive a letter from DoD that my personally identifiable information \(PII\) has been or may have been compromised?](#)
 - [What should I do if I suspect my identity has been stolen?](#)
 - [Where can I read more about federal information privacy requirements?](#)
 - [What is a Privacy Act Statement \(PAS\)?](#)
 - [What does a Privacy Act Statement tell me?](#)
 - [What is the DPCLD \(Defense Privacy & Civil Liberties Division\)?](#)
 - [What role does DPCLD play in protecting civil liberties and privacy rights?](#)
 - [What type of issues does DPCLD work on?](#)
-

What is personally identifiable information (PII)?

Personally identifiable information (PII) is any information that can be used to distinguish or trace a person's identity.

[Back to Top](#)

What are examples of personally identifiable information (PII)?

Examples of personally identifiable information (PII) include :

- Social security number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, and financial account or credit card number
- Personal address and phone number
- Biometric records such as photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, retina scan

- Biometric records such as photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, retina scan, voice signature, facial geometry
- Information that when combined with other information like that listed above which can then be used collaboratively to identify a specific individual. For example, date of birth, place of birth, race, religion, geographical indicators, employment information, medical information, education information, financial information.

[Back to Top](#)

What are the risks if personally identifiable information (PII) is misused?

Both the individual whose personally identifiable information (PII) was the subject of the misuse and the organization that maintained the PII may experience some degree of adverse effects. Depending on the type of information involved, an individual may suffer social, economic, or physical harm resulting in potential loss of life, loss of livelihood, or inappropriate physical detention. If the information lost is sufficient to be exploited by an identity thief, for example, the person may suffer from a loss of money, damage to credit, a compromise of medical records, threats, and/or harassment. The individual may also suffer tremendous losses of time and money to address the damage. Other potential harms which may result from the compromise of an individual's PII include embarrassment, improper denial of government benefits, blackmail, and discrimination.

Likewise, organizations may experience harm as a result of a loss of PII maintained by the organization. Harm may include administrative burden, remediation costs, financial losses, loss of public reputation and public trust, and legal liability.

[Back to Top](#)

Why should I be interested in the Privacy Act?

The Privacy Act of 1974 as amended at 5 U.S.C. 552a, is a code of fair information practices which mandates how Federal agencies, like the Department of Defense, maintain personally identifiable information (PII), i.e., records that uniquely identify you. The basic provisions of the Act require government agencies to:

- collect only information that is relevant and necessary to carry out an agency function;
- maintain no secret records on you;
- 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 your 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 you to see the records kept about you and provide you with the opportunity to correct inaccuracies in your records,
- allow you to find out about disclosures of your records to other agencies and persons.

The Privacy Act prohibits disclosure of these records without the written consent of the individual(s) to whom the records pertain unless one of the twelve disclosure exceptions enumerated in the Act applies. These records are held in Privacy Act [systems of records](#). A notice for each such system of records is published in the Federal Register. These notices identify the legal authority for collecting and storing the records, individuals about whom records will be collected, what kinds of information will be collected, and how the records will be used.

The Privacy Act binds only Federal agencies, and covers only records in the possession and control of Federal agencies.

[Back to Top](#)

What information is covered under the Privacy Act?

Only information held within a Federal agency's systems of records is protected under the Privacy Act.

[Back to Top](#)

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.

[Back to Top](#)

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 period of public comment before the system data collection (paper based or electronic) is started.

[Back to Top](#)

How does the government inform the public about personally identifiable information (PII) being held in its records 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. These are called [system of records notices](#) (SORNs).

[Back to Top](#)

Who can I contact if I have additional questions about the privacy of my information?

If you have additional questions about the privacy of your information, you can contact the Privacy Officer at the DoD Component holding your information. A list of DoD Component privacy officers and their contact information can be found [here](#).

[Back to Top](#)

What does it mean when a system of record notice refers to a routine use?

A routine use is an agency-approved circumstance in which a record may be shared outside of the Department of Defense (DoD) in accordance with the purpose for which the information was collected and maintained by DoD. The routine use must be included in the published notice for the system of records involved.

[Back to Top](#)

How will I know if an incident has possibly occurred that resulted in a significant compromise of my personally identifiable information (PII)?

If DoD suspects your personally identifiable information (PII) has been significantly compromised, you will be notified in writing. The notification will describe the specific data involved, the facts and circumstances surrounding the incident, the protective actions DoD is taking or you can take to mitigate against potential future harm as well as a point of contact for additional information.

What do I do if I receive a letter from DoD that my personally identifiable information (PII) has been or may have been compromised?

If you receive a notification from DoD that there has been an actual or suspected compromise of your personal information, directly contact the office sending the letter. Note that you should never give out your personal information, such as a Social Security number or financial account number over the phone unless you are certain that you are speaking with an official DoD representative. If you have any concerns over the authenticity of such a notice, contact the [specific privacy office](#) to verify.

[Back to Top](#)

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

Mitigating the harms 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](#), and our guide for [responding to identity theft](#).

[Back to Top](#)

Where can I read more about federal information privacy requirements?

- Office of Management and Budget – [Privacy Related Memoranda](#)
- Department of Justice - [Office of Privacy and Civil Liberties](#)
- Federal Trade Commission - [Identity Theft](#)
- Department of Health and Human Services – [Health Insurance Portability and Accountability Act \(HIPAA\) Privacy Rule](#)

[Back to Top](#)

What is a Privacy Act Statement (PAS)?

When a Federal agency requests that you provide personal information (name, date of birth, social security number, etc) for a system of records, regardless of the method used to collect the information (i.e., forms, personal or telephonic interview, etc), a Privacy Act Statement (PAS) is required. If the information requested will not be included in a system of records, a PAS is not required.

[Back to Top](#)

What does a Privacy Act Statement tell me?

In general the Privacy Act Statement describes

- **Authority.** The Federal law or Executive Order that allows the collection.
- **Purpose.** How the collected information will be used.
- **Routine Uses.** Agency approved circumstances in which a record may be shared outside of the agency in accordance with the purpose for which the information was collected and maintained by the agency.
- **Disclosure.** Whether or not the disclosure of information is "Voluntary" or "Mandatory". It is only appropriate to cite "Mandatory" when a Federal Law or Executive Order of the President specifically imposes a requirement to furnish the information and provides a penalty for

failure to do so. If furnishing information is a condition for granting a benefit or privilege voluntarily sought by the individual, it is voluntary for the individual to give the information.

[Back to Top](#)

What is the DPCLD (Defense Privacy & Civil Liberties Division)?

The DPCLD combines DoD's Defense Privacy Office, which was created in 1975 to implement the Privacy Act of 1974, and the Civil Liberties Office, which was created in 2009 to implement the Implementing Recommendations of the 9/11 Commission Act of 2007.

The mission of the office is "To implement the Department of Defense's Privacy and Civil Liberties programs through advice, monitoring, official reporting, and training."

[Back to Top](#)

What role does DPCLD play in protecting civil liberties and privacy rights?

DPCLD assumes an active role in protecting the civil liberties and privacy rights of U.S. Armed Forces service members, the DoD workforce, U.S. persons, and lawfully admitted aliens. DPCLD advises the Department of Defense's senior leadership on issues impacting privacy and civil liberties, including the proposed development of new policies, programs and activities. In addition, DPCLD is proactive in making available information papers and training for the DoD workforce to educate key decision makers on the privacy and civil liberties implications of DoD actions.

[Back to Top](#)

What types of issues does DPCLD work on?

- Cyber vetting
- Information sharing
- Self-radicalization / Internal Threat Identification & Tracking
- Don't Ask, Don't Tell
- Privately Owned Weapons on Military Installations
- Social media and networking

[Back to Top](#)

ABOUT THE OFFICE

[DoD Federal Privacy Rule](#)

[Mission and Functions](#)

[Principles](#)

[Leadership](#)

[Organization](#)

[Point of Contact](#)

AUTHORITIES AND GUIDANCE

[SYSTEM OF RECORDS NOTICES
\(SORNs\)](#)

[PRIVACY IMPACT ASSESSMENTS](#)

[MATCHING AGREEMENTS](#)

[RESOURCES](#)

[PRIVACY CONTACTS](#)

[FREQUENTLY ASKED QUESTIONS
\(FAQs\)](#)

[CIVIL LIBERTIES](#)

[IN THE NEWS](#)

[CONTACT DPCLD](#)

- [About DoD](#)
- [News](#)
- [Photos & Videos](#)
- [Military/DoD Websites](#)
- [Plain Writing Page](#)
- [Contact](#)

- [DoD Inspector General](#)
- [Link Disclaimer](#)
- [Recovery Act](#)
- [FOIA](#)
- [USA.gov](#)
- [No FEAR Act](#)

- [Join the Military](#)
- [DoD Careers](#)
- [Privacy & Security](#)
- [Web Policy](#)
- [DoD Section 508](#)
- [Open Government Page](#)
- [Site Map](#)