



# Department of Defense **DIRECTIVE**

**NUMBER 5400.11**  
October 29, 2014

---

---

DCMO

SUBJECT: DoD Privacy Program

References: See Enclosure 1

1. PURPOSE. This directive:

a. Reissues DoD Directive (DoDD) 5400.11 (Reference (a)) to update the established policies and assigned responsibilities of the DoD Privacy Program pursuant to section 552a of Title 5, United States Code (U.S.C.) (also known and referred to in this directive as “The Privacy Act” (Reference (b))) and Office of Management and Budget (OMB) Circular No. A-130 (Reference (c)).

b. Authorizes the Defense Privacy Board and the Defense Data Integrity Board.

c. Authorizes DoD 5400.11-R (Reference (d)) to provide guidance on The Privacy Act; prescribes uniform procedures for implementation of and compliance with the DoD Privacy Program.

d. Delegates authorities and responsibilities for the effective administration of the DoD Privacy Program.

2. APPLICABILITY

a. This directive applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this directive as the “DoD Components”).

b. For the purposes of subsection (i), “Criminal penalties,” of The Privacy Act, any DoD contractor and any employee of such a contractor will be considered to be an employee of DoD when DoD provides by a contract for the operation by or on behalf of DoD of a system of records to accomplish a DoD function. DoD will, consistent with its authority, cause the requirements of section (m) of The Privacy Act to be applied to such systems.

3. POLICY. It is DoD policy that:

a. An individual's privacy is a fundamental legal right that must be respected and protected.

(1) The DoD's need to collect, use, maintain, or disseminate (also known and referred to in this directive as "maintain") personally identifiable information (PII) about individuals for purposes of discharging its statutory responsibilities will be balanced against their right to be protected against unwarranted privacy invasions.

(2) The DoD protects individual's rights, consistent with federal laws, regulations, and policies, when maintaining their PII.

(3) DoD personnel and DoD contractors have an affirmative responsibility to protect an individual's privacy when maintaining his or her PII.

(4) Consistent with section 1016(d) of Public Law 108-458 (Reference (e)) and section 1 of Executive Order 13388 (Reference (f)), the DoD will protect information privacy and provide other protections relating to civil liberties and legal rights in the development and use of the information sharing environment.

b. The DoD establishes rules of conduct for DoD personnel and DoD contractors involved in the design, development, operation, or maintenance of any system of records. DoD personnel and DoD contractors will be trained with respect to such rules and the requirements of this section and any other rules and procedures adopted pursuant to this section and the penalties for noncompliance. The DoD Rules of Conduct are established in Enclosure 2 of this directive.

c. DoD personnel and DoD contractors conduct themselves consistent with the established rules of conduct in Enclosure 2 of this directive, so that records maintained in a system of records will only be maintained as authorized by this directive and References (b) and (d).

d. DoD legislative, regulatory, or other policy proposals will be evaluated to ensure consistency with the information privacy requirements of this directive and Reference (d).

e. Pursuant to The Privacy Act, no record will be maintained on how an individual exercises rights guaranteed by the First Amendment to the Constitution of the United States (referred to in this directive as "the First Amendment" (Reference (g))), except:

(1) When specifically authorized by statute.

(2) When expressly authorized by the individual that the record is about.

(3) When the record is pertinent to and within the scope of an authorized law enforcement activity, including an authorized intelligence or administrative investigation.

f. Disclosure of records pertaining to an individual from a system of records is prohibited except with his or her consent or as otherwise authorized by References (b) and (d) or DoD

5400.7-R (Reference (h)). When DoD Components make such disclosures, the individual may, to the extent authorized by References (b) and (d), obtain a description of such disclosures from the Component concerned.

g. Disclosure of records pertaining to personnel of the National Security Agency, the Defense Intelligence Agency, the National Reconnaissance Office, and the National Geospatial-Intelligence Agency is prohibited to the extent authorized by Public Law 86-36 and section 424 of Title 10, U.S.C. (References (i) and (j)). Disclosure of records pertaining to personnel of overseas, sensitive, or routinely deployable units is prohibited to the extent authorized by section 130b of Reference (j).

h. The DoD establishes appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual about whom information is maintained.

i. Disclosure of protected health information will be consistent with DoD 6025.18-R (Reference (k)).

j. All DoD personnel and DoD contractors will be provided training pursuant to References (b) and (c).

k. PII collected, used, maintained, or disseminated will be:

(1) Relevant and necessary to accomplish a lawful DoD purpose required by statute or Executive order.

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

(3) Relevant, timely, complete, and accurate for its intended use.

(4) Protected using appropriate administrative, technical, and physical safeguards based on the media (e.g., paper, electronic) involved. Protection will ensure the security of the records and prevent compromise or misuse during maintenance, including working at authorized alternative worksites.

l. Individuals are permitted, to the extent authorized by References (b) and (d), to:

(1) Upon request by an individual, gain access to records or to any information pertaining to the individual which is contained in a system of records.

(2) Obtain a copy of such records, in whole or in part.

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

(4) Appeal a denial for a request to access or a request to amend a record.

m. Non-U.S. citizens and aliens not lawfully admitted for permanent residence may request access to and amendment of records pertaining to them; however, this directive does not create or extend any right pursuant to The Privacy Act to them.

n. System of records notices (SORNs) and notices of proposed or final rulemaking are published in the Federal Register (FR), and reports are submitted to Congress and OMB, in accordance with References (b) through (d), Volume 1 of DoD Manual 8910.01 (Reference (l)), and DoD Instruction (DoDI) 5545.02 (Reference (m)). Information about an individual maintained in a new system of records will not be collected until the required SORN publication and review requirements are satisfied.

o. All DoD personnel must make reasonable efforts to inform an individual, at their last known address, when any record about him or her is disclosed:

(1) Due to a compulsory legal process.

(2) In a manner that will become a matter of public record.

p. Individuals must be notified in a timely manner, consistent with the requirements of Reference (d), if there is a breach of their PII.

q. At least 30 days prior to disclosure of information pursuant to subparagraph (e)(4)(D) (routine uses) of The Privacy Act, the DoD will publish an FR notice of any new use or intended use of the information in the system, and provide an opportunity for interested people to submit written data, views, or arguments to the agency.

r. Computer matching programs between the DoD Components and federal, State, or local governmental agencies are conducted in accordance with the requirements of References (b) through (d).

s. The DoD will publish in the FR notice any establishment or revision of a matching program at least 30 days prior to conducting such program of such establishment or revision if any DoD Component is a recipient agency or a source agency in a matching program with a non-federal agency.

4. RESPONSIBILITIES. See Enclosure 3.

5. INFORMATION COLLECTION REQUIREMENTS

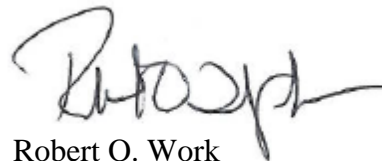
a. The DoD Privacy Act Program reporting requirements and the Biennial Matching Activity Report, referred to in paragraph 2i of Enclosure 3 of this directive, are prescribed in Reference (d).

b. The quarterly Section 803 report, referred to in paragraph 2i of Enclosure 3 of this directive, is prescribed in paragraph 6a of DoDI 1000.29 (Reference (n)) and sections 2000ee and 2000ee-1 of Title 42, U.S.C. (Reference (o)).

c. The reports directed by the Director, Defense Privacy and Civil Liberties Office (DPCLC), referred to in paragraph 4k of Enclosure 3 of this directive, have been assigned report control symbol DD-DA&M(A)1379 in accordance with the procedures in Reference (m).

6. RELEASABILITY. **Cleared for public release.** This directive is available on the Internet from the DoD Issuances Website at <http://www.dtic.mil/whs/directives>.

7. EFFECTIVE DATE. This directive is effective October 29, 2014.



Robert O. Work  
Deputy Secretary of Defense

Enclosures

1. References
2. Rules of Conduct
3. Responsibilities
4. Privacy Boards

Glossary

ENCLOSURE 1

REFERENCES

- (a) DoD Directive 5400.11, "DoD Privacy Program," May 8, 2007, as amended (hereby cancelled)
- (b) Section 552a of Title 5, United States Code (also known as "the Privacy Act" as amended)
- (c) Office of Management and Budget Circular No. A-130, "Management of Federal Information Resources," February 8, 1996
- (d) DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
- (e) Public Law 108-458, "The Intelligence Reform and Terrorism Prevention Act of 2004," December 17, 2004
- (f) Executive Order 13388, "Further Strengthening the Sharing of Terrorism Information to Protect Americans," October 25, 2005
- (g) U.S. Constitution Amendment I
- (h) DoD 5400.7-R, "DoD Freedom of Information Act Program," September 4, 1998, as amended
- (i) Public Law 86-36, "National Security Agency-Officers and Employees," May 29, 1959
- (j) Title 10, United States Code
- (k) DoD 6025.18-R, "DoD Health Information Privacy Regulation," January 24, 2003
- (l) DoD Manual 8910.01, "DoD Information Collections Manual: Procedures for DoD Internal Information Collections," June 30, 2014
- (m) DoD Instruction 5545.02, "DoD Policy for Congressional Authorization and Appropriations Reporting Requirements," December 19, 2008
- (n) DoD Instruction 1000.29, "DoD Civil Liberties Program," May 17, 2012
- (o) Title 42, United States Code
- (p) Office of Management and Budget Memorandum M-05-08, "Designation of Senior Agency Officials for Privacy," February 11, 2005
- (q) DoD Directive 5105.53, "Director of Administration and Management (DA&M)," February 26, 2008
- (r) Deputy Secretary of Defense Memorandum, "Reorganization of the Office of the Deputy Chief Management Officer," July 11, 2014
- (s) DoD Directive 5500.01, "Preparing, Processing, and Coordinating Legislation, Executive Orders, Proclamations, Views Letters, and Testimony," June 15, 2007
- (t) Office of Management and Budget Memorandum M-06-15, "Safeguarding Personally Identifiable Information," May 22, 2006
- (u) DoD Directive 5100.03, "Support to the Headquarters of Combatant and Subordinate Unified Commands," February 9, 2012

ENCLOSURE 2

RULES OF CONDUCT

In accordance with section (e)(9) of The Privacy Act, this enclosure provides DoD rules of conduct for the development, operation, and maintenance of systems of records. DoD personnel and DoD contractor personnel will:

- a. Take action to ensure that any PII contained in a system of records that they access and use to conduct official business will be protected so that the security and confidentiality of the information is preserved.
- b. Not disclose any PII contained in any system of records, except as authorized by The Privacy Act, or other applicable statute, Executive order, regulation, or policy. Those willfully making any unlawful or unauthorized disclosure, knowing that disclosure is prohibited, may be subject to criminal penalties or administrative sanctions.
- c. Report any unauthorized disclosures of PII from a system of records to the applicable Privacy point of contact (POC) for the respective DoD Component.
- d. Report the maintenance of any system of records not authorized by this directive to the applicable Privacy POC for the respective DoD Component.
- e. Minimize the collection of PII to that which is relevant and necessary to accomplish a purpose of the DoD.
- f. Not maintain records describing how any individual exercises rights guaranteed by the First Amendment, except:
  - (1) When specifically authorized by statute.
  - (2) When expressly authorized by the individual that the record is about.
  - (3) When the record is pertinent to and within the scope of an authorized law enforcement activity, including authorized intelligence or administrative activities.
- g. Safeguard the privacy of all individuals and the confidentiality of all PII.
- h. Limit the availability of records containing PII to DoD personnel and DoD contractors who have a need to know in order to perform their duties.
- i. Prohibit unlawful possession, collection, or disclosure of PII, whether or not it is within a system of records.

j. Ensure that all DoD personnel and DoD contractors who either have access to a system of records or develop or supervise procedures for handling records in a system of records are aware of their responsibilities and are properly trained to safeguard PII being maintained under the DoD Privacy Program.

k. Prepare any required new, amended, or altered SORN for a given system of records and submit the SORN through their DoD Component Privacy POC to the Director, DPCLCLO, for coordination and submission for publication in the FR.

l. Not maintain any official files on individuals, which are retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual, also known as a system of records, without first ensuring that a notice has been published in the FR. Any official who willfully maintains a system of records without meeting the publication requirements as prescribed by this directive and The Privacy Act may be subject to criminal penalties or administrative sanctions.

m. Maintain all records in a mixed system of records as if all the records in such a system are subject to The Privacy Act.



ENCLOSURE 3

RESPONSIBILITIES

1. DEPUTY CHIEF MANAGEMENT OFFICER OF THE DEPARTMENT OF DEFENSE (DCMO). The DCMO:

a. Serves as the Senior Agency Official for Privacy (SAOP) for the DoD. These duties, in accordance with OMB Memorandum M-05-08 (Reference (p)), include:

(1) Ensuring DoD implementation of information privacy protections, including full compliance with federal laws, regulations, and policies relating to information privacy.

(2) Overseeing, coordinating, and facilitating DoD privacy compliance efforts.

(3) Ensuring that DoD personnel and DoD contractors receive appropriate training and education programs regarding the information privacy laws, regulations, policies, and procedures governing DoD-specific procedures for handling of PII.

b. Provides rules of conduct and policy for, and coordinates and oversees administration of, the DoD Privacy Program to ensure compliance with policies and procedures in References (b) and (c).

c. Publishes Reference (d) and other guidance to ensure timely and uniform implementation of the DoD Privacy Program.

d. Serves as the chair of the Defense Privacy Board and the Defense Data Integrity Board.

e. As requested, ensures that guidance, assistance, and subject matter expert support are provided to the Combatant Command privacy officers in the implementation and execution of and compliance with the DoD Privacy Program.

f. Acts as The Privacy Act Access and Amendment appellate authority for OSD and the Office of the Chairman of the Joint Chiefs of Staff when an individual is denied access to or amendment of records pursuant to The Privacy Act, DoDD 5105.53 (Reference (q)), and Deputy Secretary of Defense Memorandum (Reference (r)).

2. DIRECTOR, DPCLC. Under the authority, direction, and control of the DCMO, through the Director for Compliance and Oversight, the Director, DPCLC:

a. Ensures that laws, policies, procedures, and systems for protecting individual privacy rights are implemented throughout DoD.

b. Oversees and provides strategic direction for the DoD Privacy Program.

- c. Assists the DCMO in performing the responsibilities in section 1 of this enclosure.
- d. Reviews DoD legislative, regulatory, and other policy proposals that contain information privacy issues relating to how the DoD keeps its PII. These reviews must include any proposed legislation, testimony, and comments having privacy implications in accordance with DoDD 5500.01 (Reference (s)).
- e. Reviews proposed new, altered, and amended systems of records. Submits required SORNs for publication in the FR and, when required, provides advance notification to OMB and Congress consistent with References (b) through (d).
- f. Reviews proposed DoD Component privacy exemption rules. Submits the exemption rules for publication in the FR, and submits reports to OMB and Congress consistent with References (b) through (d).
- g. Develops, coordinates, and maintains all DoD computer matching agreements. Submits required match notices for publication in the FR and provides advance notification to OMB and Congress consistent with References (b) through (d).
- h. Provides guidance, assistance, and support to the DoD Components in their implementation of the DoD Privacy Program to ensure that:
  - (1) All requirements developed to maintain PII conform to the DoD Privacy Program standards.
  - (2) Appropriate procedures and safeguards are developed and implemented to protect PII when it is collected, used, maintained, or disseminated in any media.
  - (3) Specific procedures and safeguards are developed and implemented when PII is collected and maintained for research purposes.
- i. Compiles data in support of the DoD Chief Information Officer (DoD CIO) submission of the Federal Information Security Management Act Privacy Reports, pursuant to OMB Memorandum M-06-15 (Reference (t)); the Biennial Matching Activity Report to OMB, in accordance with References (c) and (d); the quarterly Section 803 report in accordance with sections 2000ee and 2000ee-1 of Reference (o); and other reports as required.
- j. Reviews and coordinates on DoD Component privacy program implementation rules to ensure they are in compliance with the DoD-level guidance.
- k. Provides operational and administrative support to the Defense Privacy Board and the Defense Data Integrity Board.

3. GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE (GC DoD). The GC DoD:
  - a. Provides advice and assistance on all legal matters related to the administration of the DoD Privacy Program.
  - b. Appoints a designee to serve as a member of the Defense Privacy Board and the Defense Data Integrity Board.
  - c. When a DoD Privacy Program group is created, appoints a designee to serve as a member.
  
4. DoD COMPONENT HEADS. The DoD Component heads:
  - a. Provide adequate funding and personnel to establish and support an effective DoD Privacy Program.
  - b. Establish DoD Component-specific procedures in compliance with this directive and publish these procedures as well as rules of conduct in the FR.
  - c. Establish and implement appropriate administrative, physical, and technical safeguards and procedures prescribed in this directive and other DoD Privacy Program guidance.
  - d. Ensure Component compliance with supplemental guidance and procedures in accordance with all applicable federal laws, regulations, policies, and procedures.
  - e. Appoint a Component senior official for privacy (CSOP) to support the SAOP in carrying out the SAOP's duties identified in Reference (p).
  - f. Appoint a Component privacy officer to administer the DoD Privacy Program, on behalf of the CSOP.
  - g. Ensure DoD personnel and DoD contractors having primary responsibility for implementing the DoD Privacy Program receive appropriate privacy training. This training must be consistent with the requirements of Reference (d) and will address the provisions of this directive and References (b) through (d).
  - h. Ensure that all DoD Component legislative, regulatory, or other policy proposals are evaluated to ensure consistency with the information privacy requirements of this directive and Reference (d).
  - i. Assess the impact of technology on the privacy of PII and, when feasible, adopt privacy-enhancing technology to:
    - (1) Preserve and protect PII contained in a DoD Component system of records.
    - (2) Audit compliance with the requirements of this directive and Reference (d).

j. Ensure that officials who have specialized knowledge of the DoD Privacy Program periodically review Component implementation of and compliance with the DoD Privacy Program.

k. Submit reports, consistent with the requirements of Reference (d), in accordance with References (b) and (c), and as otherwise directed by the Director, DPCLCLO.

5. SECRETARIES OF THE MILITARY DEPARTMENTS. In addition to the responsibilities in section 4 of this enclosure, the Secretaries of the Military Departments provide program and financial support to the Combatant Commands as identified in DoDD 5100.03 (Reference (u)) to fund, without reimbursement, the administrative and logistic support required by combatant and subordinate unified command headquarters to perform their assigned missions effectively.

ENCLOSURE 4

PRIVACY BOARDS

1. THE DEFENSE PRIVACY BOARD

a. Membership. The Board consists of:

(1) Voting Members. Representatives designated by the Secretaries of the Military Departments and the following officials or their designees:

- (a) The DCMO, who serves as the chair.
- (b) The Director, DPCLO.
- (c) The Director for Privacy, DPCLO, who serves as the Executive Secretary and as a member.
- (d) The Under Secretary of Defense for Personnel and Readiness.
- (e) The Assistant Secretary of Defense for Health Affairs.
- (f) The DoD CIO.
- (g) The Director, Defense Manpower Data Center.
- (h) The Director, Executive Services Directorate, Washington Headquarters Services (WHS).
- (i) The GC DoD.
- (j) The Chief of the National Guard Bureau.

(2) Non-Voting Members. Non-voting members are the Director, Enterprise Information Technology Services Directorate (EITSD), WHS; and the representatives designated by Defense Agency and DoD Field Activity directors.

b. Responsibilities. The Board:

(1) Serves as the primary DoD policy forum for matters involving the DoD Privacy Program, meeting as necessary to address issues of common concern to ensure that consistent policy is adopted and followed by the DoD Components. The Board issues advisory opinions, as necessary, on the DoD Privacy Program to promote uniform and consistent application of References (b) through (d).

(2) Establishes and convenes committees as necessary.

(3) Establishes working groups whose membership is composed of DoD Component privacy officers and others as necessary.

## 2. THE DEFENSE DATA INTEGRITY BOARD

a. Membership. The Board consists of:

(1) The DCMO, who serves as the chair.

(2) The Director, DPCLCLO.

(3) The Director for Privacy, DPCLCLO, who serves as the Executive Secretary.

(4) The representatives designated by the Secretaries of the Military Departments; the DoD CIO; the GC DoD; the Inspector General of the Department of Defense, who is a non-voting advisory member; the Director, EITSD; and the Director, Defense Manpower Data Center.

b. Responsibilities. The Board:

(1) Oversees and coordinates, consistent with the requirements of References (b) through (d), all computer matching agreements involving personal records contained in systems of records maintained by the DoD Components.

(2) Reviews and approves all computer matching agreements between the DoD and other federal, State, or local governmental agencies, as well as any memorandums of understanding, when the match is internal to the DoD. This review ensures that, in accordance with References (b) through (d), appropriate procedural and due process requirements are established before engaging in computer matching activities.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

CSOP	Component senior official for privacy
DCMO	Deputy Chief Management Officer of the Department of Defense
DoD CIO	DoD Chief Information Officer
DoDD	DoD Directive
DoDI	DoD Instruction
DPCLCLO	Defense Privacy and Civil Liberties Office
EITSD	Enterprise Information Technology Services Directorate
FR	Federal Register
GC DoD	General Counsel of the Department of Defense
OMB	Office of Management and Budget
PII	personally identifiable information
POC	point of contact
SAOP	Senior Agency Official for Privacy
SORN	system of records notice
U.S.C.	United States Code
WHS	Washington Headquarters Services

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purpose of this directive.

breach. A 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.

computer matching. The computerized comparison of two or more automated systems of records or a system of records with non-federal records. Manual comparisons are not covered.

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.

DoD 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.

DoD personnel. Service members and federal civilian employees.

information sharing environment. Defined in Reference (e).

individual. A living person who is a U.S. citizen or an alien lawfully admitted for permanent residence. The parent of a minor or the legal guardian of any individual also may act on behalf of an individual, except as otherwise provided in Reference (d). 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 persons employed by such organizations or entities are "individuals" when acting in a personal capacity (e.g., security clearances, entitlement to DoD privileges or benefits).

maintain. The collection, maintenance, use, or dissemination of records contained in a system of records.

mixed system of records. Any system of records that contains information about individuals as defined by the Privacy Act and non-U.S. citizens and/or aliens not lawfully admitted for permanent residence.

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. For purposes of this issuance, the term PII also includes personal information and information in identifiable form.

protected health information. Defined in Reference (k).

record. Any item, collection, or grouping of information in any media (e.g., paper, electronic), about an individual that is maintained by a DoD Component, including, but not limited to, education, financial transactions, medical history, criminal or employment history, and that contains the name, or identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint, a voice print, or a photograph.

SORN. A notice published in the FR that constitutes official notification to the public of the existence of a system of records.

system of records. A group of records under the control of a DoD 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.