



PRIVACY IMPACT ASSESSMENT (PIA)

For the

USMC Mass Communications Tool
Headquarters Marine Corps Personal and Family Readiness Division

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

- (1) Yes, from members of the general public.
- (2) Yes, from Federal personnel* and/or Federal contractors.
- (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.
- (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- New DoD Information System
- New Electronic Collection
- Existing DoD Information System
- Existing Electronic Collection
- Significantly Modified DoD Information System

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- Yes, DITPR Enter DITPR System Identification Number
- Yes, SIPRNET Enter SIPRNET Identification Number
- No

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- Yes
- No

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

- Yes
- No

If "Yes," enter Privacy Act SORN Identifier

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: <http://www.defenselink.mil/privacy/notices/>

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

Yes

Enter OMB Control Number

Enter Expiration Date

No

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

10 U.S.C. 5013; Secretary of the Navy; 10 U.S.C. 5041, Headquarters, U.S. Marine Corps; MCO 1754.6A and NAVMC 1754.6A, USMC Marine Corps Community Services (MCCS) Marine Corps Family Team Building (MCFTB); and E.O. 9397 (SSN).

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

1. Introduction: The desired outcome of Marine Corps Family Team Building (MCFTB) is family readiness. Family readiness is defined as families who are prepared and equipped with the skills and tools to successfully meet the challenges of the military lifestyle. The HQ USMC Marine Corps Community Services (MCCS) was tasked to acquire and implement a Mass Communications Tool as part of the Commandant's Marine Corps Family Team Building Initiatives. The Marine Corps Family Team Building (MCFTB) Branch of MCCS has implemented a mass communication capability hosted by a third party contractor. The solution is currently deployed to 18 Marine Corps installations around the world. The primary user of the system is over 400 Family Readiness Officers in service for every Marine registered in the system. The system is currently populated with over 128,000 contacts with a target capacity for 1,000,000 contacts. The Contractor provides software as a service (SaaS) and hosts all data on an MCCS database. Currently, MCCS employs a version of the MCT that is undergoing a custom application upgrade and will allow Marines to register and to edit their personal profiles and contacts via the Marine-on-Line (MOL). The data captured and stored on the MCT is categorically PII.

2. Background:

a. A MCFTB Functionality Assessment (FA) was held in May 2007 that indicated our current family readiness programs do not adequately support an increased level of family readiness and must be adapted to meet the Commandant's wartime footing mandate.

b. The Inspector General of the Marine Corps (IGMC) conducted a Family Readiness Assessment at various installations around the Marine Corps. This assessment further validated the FA findings that today's family readiness programs are structured to peacetime model with no dedicated military infrastructure and an excessive reliance on volunteers.

c. Previously the method of unit communication is volunteer dependent and relies on trained Key Volunteers to relay official information from the Commander to the families, via a traditional call tree. Due to the ratio of volunteers to unit families, the call tree proved to be labor intensive and at times ineffective. The Family Readiness Officers (FROs) were responsible for communicating with the families of Single Marines.

d. As a result of the FA, an expansion of the definition of the family to broaden the scope of the communication for commanders to include extended family members. In the new model unit volunteers will not take part in communication between the Commander and families. The FRO will provide all unit communication to families and thus the need for an effective and efficient tool which will provide instant feedback on recipient verification of the unit's family contact information. HQMC MR has employed full-time FROs to implement an electronic Mass Communication tool. The FRO is able to distribute official command information quickly and accurately and receives instant feedback regarding inconsistencies in the unit's family contact information.

3. Purpose: The purpose of this capability is to provide a comprehensive solution for Marine Commanders and their designated staff members (FRO) to communicate from a single location or multiple locations to a select audience or audiences of Marines and Marine family members. The requirement demands the implementation of a proven and reliable technology that enables Marine Corps Commanders to communicate with Marine family members accurately, rapidly, efficiently and in mass. The system provides the means for Marines to register with their personal profiles and to create the profiles for as many as four additional contacts, to include family members or other important contacts. The solution allows mass notification-capability to send electronic messages that can be received via telephone, cell phone, email, text message, etc. A contract was awarded to design, develop, deliver and maintain the Mass Communication Tool throughout its life cycle.

4. PII Data Currently Collected; System of Record:

- a. First name
- b. Middle Initial
- c. Last Name
- d. SSN Last Four (military member only)
- e. Home Address
- f. Work Address

g. Telephone Numbers

h. E-mail Address

i. Relationship

j. The DOB (military member only) will be added to the database structure with the Customized Application Upgrade scheduled for March 2010. The purpose of this addition is to provide unique identification options while eliminating the storage and use of the SSN Last Four in the current version of the MCT.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

The current version of the MCT implements a manual means for initial data collection from each Marine. The Marine does not interface directly with the MCT at any stage during its use. The primary user interface is accomplished by the Family Readiness Officer (FRO). Over 400 FROs are employed down to Battalion Command level across the entire Corps. Each FRO is a direct report to their assigned unit Commander. The FRO collects profile and contact information from each Marine IAW routine unit staff action to process a Marine into the unit. The Marine meets face to face with the FRO, acquires a standard paper form to hand print personal profile information and required contact information for no more than four contacts of choice. If the Marine decides to participate and in turn provides the completed form to the FRO, upon receiving the form the FRO will enter the information provided into a standard formatted spreadsheet. The FRO performs all tasks on a government issued workstation connected to a government protected network. FRO access is granted with CAC enabled PKI Authentication. The FRO completes the spreadsheet with information for multiple Marines and only those Marines the FRO is responsible. From the spreadsheet the FRO creates a .csv flat file to transfer by secure protocol to the contractor hosted MCT database. FRO access to the MCT is granted with authentication via user name and password. The risks associated with this process begin with the paper copy of information provided to the FRO by the Marine and the risks continue with the care and maintenance of this document and the spreadsheet. The risk is mitigated first and foremost with training and certification of every FRO on the Privacy ACT and PII certification. The role and responsibility of FRO is granted to only those who satisfy the certification. The risk to PII compromise or inappropriate dissemination is further mitigated by document management IAW USMC standard procedures for handling and securing confidential information. The documents are securely stored and managed in the unit area.

The future version of the MCT, scheduled for delivery in 2010, will provide electronic entry of PII by each Marine via Marine-on-Line (MOL) as the primary means for initial data entry and anytime editing. MOL access will require user name/password and access to MCT and will require CAC enabled PKI Authentication or MOL user name and password. The future version of MCT will be positioned to comply with MOL future for CAC only access. The future version of MCT will also retain an improved spreadsheet upload for the FRO to accommodate scenarios when Marines cannot make the entry themselves or scenarios that demand mass uploads by the FRO.

For both the current and future versions of the MCT the PII collected and maintained on the MCT database and system infrastructure will be at very low risk. The contractor's infrastructure is hardened according to industry best practices and layered in accordance with a defense in depth strategy to mitigate any threat that might exist. The MCT and system infrastructure was previously accredited by a significant government agency recognized by the USMC C4/IA. The contractor's infrastructure is designed and deployed according to industry best practices as outlined in ISO 17799 (ISO/IEC 27002) Information Technology Security Techniques. Our infrastructure is maintained at Communications CyberCenters which are independently certified annually to comply with physical and procedural security standards by SAS70 Type II audit.

Following are key items implement at Communications CyberCenters:

- 24/7 on-site hosting system and network monitoring
- 24/7 CyberCenter facility customer support and monitoring
- 24/7 security staff
- Strictly enforced security procedures
- Photo ID required for building access
- Sophisticated computerized access control system
- Card key and biometrics scan required for collocation space access
- Video surveillance at all entrances and every aisle (60-day, on-site tape retention)

• Locked racks and cabinets with local key management

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

Within the DoD Component.

Specify. PII is only shared within our DoD Component, Family Readiness Officers, Commanders and Staff of Major and Subordinate USMC Commands and with our hosting contractor.

Other DoD Components.

Specify. []

Other Federal Agencies.

Specify. []

State and Local Agencies.

Specify. []

Contractor (Enter name and describe the language in the contract that safeguards PII.)

Specify. The Contractor agrees to –

1. Privacy Act

a. Comply with the Privacy Act 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies:

(1) The systems of records; and

(2) The design, development, or operation work that the Contractor is to perform;

b. Include the privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the design, development, or operation of a system of records on individuals that is subject to the Act; and

c. Include this clause, including this subparagraph c., in all subcontracts awarded under this contract which requires the design, development, or operation of such a system of records.

d. In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a system of records on individual's to accomplish an agency function. For purposes of the Act, when the contract is for operation of a system of records on individuals to accomplish an agency function, the Contractor and any employee of the Contractor is considered to be an employee of the agency.

"Operation of a system of records," as used in this clause, means performance of any of the activities associated with maintaining the system of records, including the collection, use and dissemination of records.

(1). "Record," as used in this clause, means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to; education, financial transactions, medical history, and criminal or employment history and that contains the person's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint or voiceprint or a photograph.

(2). Privacy Act Data shall not be stored on any mobile storage device i.e. laptops, thumb drives, portable hard drive, etc.

(3). If transmitting Privacy Act Data, files will be encrypted, password protected, or sent via secure FTP.

3. For Internet Access the contract states:

a. Internet access and control measure certifiable in accordance with USMC MCCS policies and regulations [Marine Corps Order (MCO) P1700.27B (<http://www.usmc.mil/directiv.nsf/Pdocuments?openview&count=5000&start=1>), Department of Defense Directive (DoDD) 8500. 1 (<https://acc.dau.mil/CommunityBrowser.aspx?id=37475&lang=en-US>), and Department of Defense Instructions (DoDI) 8500.2 (<http://www.dtic.mil/whs/directives/corres/html/850002.htm>)].

b. Adequate application administration tools for the FRO and System Administrators.

c. Directory/Database solution that is scalable to the grown and needs of the USMC, and is certifiable for security standards in accordance with USMC MCCS policies and regulations [Marine Corps Order (MCO) P1700.27B (<http://www.usmc.mil/directiv.nsf/Pdocuments?openview&count=5000&start=1>), Department of Defense Directive (DoDD)8500.0 (<https://acc.dau.mil/CommunityBrowser.aspx?id=37475&lang=en-US>), and Department of Defense Instructions (DoDI) 8500.2 (<http://www.dtic.mil/whs/directives/corres/html/850002.htm>)].

4. RIGHTS IN DATA—MCT

a. In the event that the Contractor delivers technical data or computer software to the MCCS, the Contractor will grant the MCCS a license to use that data or software providing that the Contractor and MCCS agree on the terms and conditions that may be provided with that data or software. The foregoing applies to commercial off the shelf (COTS) software as well as to any delivered software that may be developed or modified to meet the MCCS requirements.

b. The contractor acknowledges and agrees that it shall have no right, title, claim or interest in any of the information or data provide to the Contractor by MCCS or users, which may include specifications, designs, plans, drawings, software, computer systems, prototype or other information, to include personal information, which may be disclosed to the Contractor in the course of providing services hereunder.

c. Release and use Restrictions. Except as otherwise specifically provided for in this contract, the Contractor shall not sue or release for purposes other than the performance of this contact, information provide to the Contractor by MCCS or users, not shall the contractor release, reproduce, distribute, or publish any data produced in performance of this contract, or authorize others to do so, without written permission of the Contracting Officer.

Other (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

Yes No

(1) If "Yes," describe method by which individuals can object to the collection of PII.

Yes. The Marine can object to collection of their PII. The current version of the MCT requires the Marine to complete a standard form provided by the FRO. The form includes the Privacy Act statement and the opportunity for the Marine to opt out and not participate.

The future version of the MCT provides the opportunity for the Marine to object to the collection of their PII on the input screen of the tool.

(2) If "No," state the reason why individuals cannot object.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

Yes No

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

Yes. Marines do have the opportunity to consent to the specific use of their PII. Consent is given by each Marine upon their completion and signing the consent form provided. If they do not consent their PII is not captured and will not be stored in the MCT system. The form they are provided states that PII will be used solely for matters pertaining to the Unit Personal and Family Readiness Program (UPFRP). PII is used only within the MCT system for identification of the Marine, the association of the Marine with their assigned unit and for maintaining their relationship with their personal contacts.

In the future version of the MCT the Marine must accept the Terms of Use (TOU) prior to saving their record and the TOU will include acceptable use of the system in accordance with MCCS policy and guidelines.

(2) If "No," state the reason why individuals cannot give or withhold their consent.



k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

- Privacy Act Statement
- Privacy Advisory
- Other
- None

Describe each applicable format.

The Privacy Statement is printed on the form provided to the Marine for PII collection. The future version of the MCT will display the website equivalent of the Privacy Statement. Below is the actual content of the MCT Contact Data Sheet with Privacy Statement currently in use.

Mass Communication Tool Contact Data Sheet:

The information requested below is being collected for use within the Marine Corps' Mass Communication Tool. The Tool is currently being fielded across the Marine Corps, and will be used as a mean of communicating with Marines and their families, especially those in a deployed status. The Tool will be used by the Family Readiness Officer and has the options for sending notifications via email, phone, or text messaging. No classified or casualty information will be distributed via this tool. Every Marine has the ability to add up to four individual contacts. The data collected will be stored securely within the Mass Communication Tool and will not be shared with any outside sources; the data will only be used for notifications associated to your Command. Please be sure to write legibly, so we can transfer the data into the tool correctly.

MARINE CORPS FAMILY READINESS PROGRAM MASS COMMUNICATION TOOL PRIVACY ACT STATEMENT AUTHORITY: 10 USC 5013; EO 9397.10 USC 5041 PRINCIPAL PURPOSE(S): to obtain information needed for the Family Readiness Program Mass Communication Tool that will enable Marine Corps Commanders and their designated staff members to communicate in an accurate, rapid, and efficient manner with Marine family members and others designated by the Marine en mass. The Tool has the options for sending notifications via email, phone, or text messaging. No classified or casualty information will be distributed via this tool.

ROUTINE USES(S): None.

DISCLOSURE: Voluntary; however, if an enrollee fails to furnish information requested on this form it may impair Commanders' and their staff members' ability to communicate important information to your family members or others designated by you to receive such information, particularly when you may be in a deployed status. Enrollees must provide the last four digits of the Social Security Number (SSN) in order to identify them and their selected contacts.

I authorize the following individuals to be contacted on my behalf: Sign

MARINE INFORMATION: UIC:

First Name and MI:
 Last Name:
 Last four (4) of SSN:
 Address (street number/name):
 Apt #:
 City:
 State:
 Country:
 Work E-mail Address:
 Home E-Mail:
 Alternate E-Mail:
 Work Cell Phone:
 Personal Cell Phone:
 Business Phone & Ext.
 Home Phone:
 Text Device (unlimited):

Text Device (limited):
SMS Device:
ZIP:
Preferred Language:

NOTE: All contacts must be 18 years of age or older to be entered into the Mass Communication Tool unless the contact is a spouse.

CONTACT #1 - #4:
First Name and MI:
Last Name:
Contact Code :
Address (Street/Number):
Apt No.
City
State
Country
Work E-mail Address:
Home E-Mail:
Alternate E-Mail:
Work Cell Phone:
Personal Cell Phone:
Business Phone & Ext.
Home Phone:
Text Device (unlimited):
Text Device (limited):
SMS Device:
ZIP
Preferred Language:

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.

SECTION 4: REVIEW AND APPROVAL SIGNATURES

Prior to the submission of the PIA for review and approval, the PIA must be coordinated by the Program Manager or designee through the Information Assurance Manager and Privacy Representative at the local level.

Program Manager or Designee Signature

	BURKETT.FRANKLIN.J.1177840684 <small>Digitally signed by BURKETT.FRANKLIN.J.1177840684 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=BURKETT.FRANKLIN.J.1177840684 Date: 2009.08.27 15:21:26 -0400</small>
Name:	Franklin J. Burkett
Title:	Manager, IT, PMP
Organization:	HQ USMC MCCA
Work Telephone Number:	703-784-4017
DSN:	278-4017
Email Address:	franklin.burkett@usmc-mcca.org
Date of Review:	08/27/2009

Other Official Signature (to be used at Component discretion)

	HARRIS.RANDY.LEE.1061012237 <small>Digitally signed by HARRIS.RANDY.LEE.1061012237 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USMC, cn=HARRIS.RANDY.LEE.1061012237 Date: 2009.09.02 10:01:30 -0400</small>
Name:	Randy L. Harris
Title:	Chief Information Security Officer (CISO)
Organization:	HQ USMC MCCA
Work Telephone Number:	703-432-2974
DSN:	378-2974
Email Address:	harrisrl@usmc-mcca.org
Date of Review:	09/01/2009

**Other Official Signature
(to be used at Component
discretion)**

Name:

Title:

Organization:

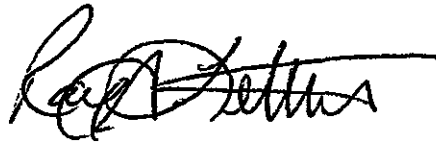
Work Telephone Number:

DSN:

Email Address:

Date of Review:

**Component Senior
Information Assurance
Officer Signature or
Designee**



Name:

Ray A. Letteer

Title:

Chief, Information Assurance (IA) Division

Organization:

HQMC Command, Control, Communications and Computers (C4) IA

Work Telephone Number:

(703) 693-3490

DSN:

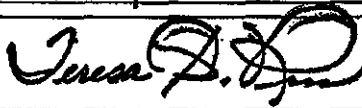
Email Address:

ray.letteer@usmc.mil

Date of Review:

9 Sep 2009

**Component Privacy Officer
Signature**



Name:

Teresa D. Ross

Title:

USMC Privacy Act/FOIA Manager

Organization:

HQMC ARSF

Work Telephone Number:

(703) 614-4008

DSN:

Email Address:

teresa.d.ross@usmc.mil

Date of Review:

9/4/2009

**Component CIO Signature
(Reviewer)**



Name: Steve Muck

Title: Privacy Team Lead

Organization: Department of the Navy Chief Information Officer (DON CIO)

Work Telephone Number: (703) 614-5987

DSN: 224-5987

Email Address: steven.muck@navy.mil

Date of Review:

21 Sep 09

**Component CIO Signature
(Reviewing Official)**



Name: Robert J. Carey

Title: Chief Information Officer

Organization: Department of the Navy Chief Information Officer (DON CIO)

Work Telephone Number: (703) 602-1800

DSN: 332-1800

Email Address: robert.carey@navy.mil

Date of Review:

9/21/09

Publishing:

Only Sections 1 and 2 of this PIA will be published. Each DoD Component will maintain a central repository of PIAs on the component's public Web site. DoD Components will submit an electronic copy of each approved PIA to the DoD CIO at: pia@osd.mil.

If the PIA document contains information that would reveal sensitive information or raise security concerns, the DoD Component may restrict the publication of the assessment to include Sections 1 and 2.

APPENDIX

Data Aggregation. Any process in which information is gathered and expressed in a summary form for purposes 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.

DoD Information System. A set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system (AIS) applications, enclaves, outsourced information technology (IT)-based processes and platform IT interconnections.

Electronic Collection. Any collection of information enabled by IT.

Federal Personnel. Officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), and individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the United States (including survivor benefits). For the purposes of PIAs, DoD dependents are considered members of the general public.

Personally Identifiable Information (PII). Information about an individual that identifies, links, relates or is unique to, or describes him or her (e.g., a social security number; age; marital status; race; salary; home telephone number; other demographic, biometric, personnel, medical, and financial information). Also, information that can be used to distinguish or trace an individual's identity, such as his or her name; social security number; date and place of birth; mother's maiden name; and biometric records, including any other personal information that is linked or linkable to a specified individual.

Privacy Act Statements. When an individual is requested to furnish personal information about himself or herself for inclusion in a system of records, providing a Privacy Act statement is required to enable the individual to make an informed decision whether to provide the information requested.

Privacy Advisory. A notification informing an individual as to why information is being solicited and how such information will be used. If PII is solicited by a DoD Web site (e.g., collected as part of an email feedback/ comments feature on a Web site) and the information is not maintained in a Privacy Act system of records, the solicitation of such information triggers the requirement for a privacy advisory (PA).

System of Records Notice (SORN). Public notice of the existence and character of a group of records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act of 1974 requires this notice to be published in the Federal Register upon establishment or substantive revision of the system, and establishes what information about the system must be included.