DHA PRIVACY AND
CIVIL LIBERTIES OFFICE
Defending Privacy

Privacy Impact Assessment Desk Reference Guide

March, 2016

Defense Health Agency (DHA)
Privacy and Civil Liberties Office
7700 Arlington Boulevard Suite 5101
Falls Church, VA 22042
703-275-6363

Colleagues:

This desk reference provides a clear and straightforward overview to guide you through the privacy impact assessment (PIA) process. The approach we use, removing all blinders and looking at the larger picture, when preparing PIAs is important to the privacy and data protection landscape.

Per Section 208 of the E-Government Act of 2002, federal agencies must conduct an analysis of how they handle personally identifiable information. Based on the requirements set forth in the E-Government Act, the Department of Defense (DoD) established the DoD Instruction 5400.16, DoD Privacy Impact Assessment (PIA) Guidance, which provides a standardized methodology for conducting PIAs. However, as humans, we are bound to have different interpretations of the requirements outlined in the laws and policies. I am hopeful that this desk reference will alleviate most differences in interpretation and understanding of the law and DoD policy for PIAs.

When you engage in writing your PIA, keep in mind that the PIA serves as a valuable tool used to help all stakeholders understand the mechanics of the information system, the information collected, the privacy concerns and risks, and the mitigation strategies for any potential privacy risks. The PIA process also allows the program manager or system owner to determine whether the information system is complaint with the E-Government Act and DoD policies regarding privacy at any point in the life cycle.

It is with great enthusiasm that I provide this desk reference for your use to sail smoothly though the PIA process. As you embark upon your journey of preparing a PIA for your information system, this is your opportunity to identify key problems and answer the hard questions.

Linda S. Thomas
Chief, DHA Privacy and Civil Liberties Office

Introduction

The Defense Health Agency (DHA) is committed to ensuring the appropriate protection of privacy and civil liberties in the course of fulfilling its missions. Privacy Impact Assessments (PIAs), which are required by Section 208 of the E-Government Act of 2002, are an important process that assists the DHA in achieving this objective. Section 208 requires all Federal government agencies to conduct PIA before developing or procuring information technology that collects, maintains, or disseminates personally identifiable information (PII) or before initiating a new collection of information that will be collected, maintained, or disseminated using information technology and that includes any PII in certain situations involving the public. Section 208 also requires Federal agencies to make their PIAs publicly available. The Department of Defense Instruction (DoDI) 5400.16, DoD Privacy Impact Assessment (PIA) Guidance provides the procedures for the completion and approval of PIAs to analyze and ensure PII in electronic form is collected, stored, protected, used, shared, and managed in a manner that protects privacy. The Chief Information Officer approves PIAs conducted by the DHA's program offices.

This guidance is designed to assist organizations under DHA to effectively conduct a PIA and how to properly document this assessment. This guidance reflects the requirements of the Section 208 of the E-Government Act and DoDI 5400.16. The Chief, DHA Privacy and Civil Liberties Office (DHA Privacy Office) encourages all program offices and system owners developing new PIAs to follow this PIA Desk Reference Guide.

References

- Section 208 of Public Law 107-347, "E-Government Act of 2002," December 17, 2002
- Office of Management and Budget (OMB) Memorandum M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," September 26, 2003
- DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance," July 14, 2015

Privacy Threshold Analysis

Some information systems will not require a full PIA. For efficiency, a system owner or program manager can be aided in making the determination of whether a full PIA is required by conducting and following a Privacy Threshold Analysis (PTA). For any information system transitioning to DHA that does not have a PIA and new information systems, a PTA should be conducted in order to determine if a full PIA is necessary.

A properly completed and approved PTA provides documentation that a system owner thought through privacy concerns whether or not a full PIA is deemed to be required. A PTA provides a foundation for a full PIA should one be required.

Upon completion of the Privacy Threshold Analysis (PTA) DHA Form 61, return the DHA Form to the DHA Privacy Office for review and determination. The completed PTA should be submitted to dha.ncr.pcl.mbx.piamail@mail.mil. Upon review, the DHA Privacy Office will return the PTA with the determination and provide further instructions.

Communication

Communication between the DHA Privacy Office and Program Office is the key to completing an effective PIA. The PIA process (see Appendix III) requires ongoing communication between the DHA Privacy Office and Program Office to ensure appropriate and timely handling of privacy concerns. The PIA process requires candid and forthcoming conversations between the DHA Privacy Office and Program Office to ensure appropriate and timely handling of privacy concerns. Addressing privacy issues publicly through a PIA builds public trust and fosters openness and transparency in the operations of the DHA.

The Section 208 of the E-Government Act requires, where practicable, that agencies make PIAs publicly available. Therefore, PIAs should be clear, unambiguous, and understandable to the public. The length and breadth of a PIA will vary according to the size and complexity of the system. The PIA should demonstrate that an in-depth analysis was conducted to ensure that privacy protections were built into the system. Some helpful tips for completing the PIA are:

- Draft PIAs from the perspective of a member of the public who knows nothing about the system, technology, or rulemaking. The PIA should be written with sufficient detail to permit the Privacy Office to analyze the privacy risks and mitigation steps.
- The PIA will be published on the DHA's web site with portions possibly published in the Federal Register. PIAs submitted to the DHA Privacy Office should be free of spelling and grammatical errors.
- Spell out each acronym the first time you use it in the document. For example, Office of Management and Budget (OMB).
- Use words, phrases, or names in the PIA that are readily known to the average person.
- Technical terms or references should be defined.
- Clearly reference projects and systems and provide explanations, if needed, to aid the general public.
- Use the complete name of reference documents. For example, references to National Institute of Science and Technology (NIST) publications and other documents should include the complete name of the reference (e.g., NIST Special Publication 800-53A, Assessing Security and Privacy Controls in Federal Information Systems and Organizations). Subsequent references may use the abbreviated format.

Desk Guide to Completing the Privacy Impact Assessment, DD Form 2930

When completing the PIA, think about the purpose of the PIA. The PIA should describe the flow of personal data so that everyone can understand the impact that the new system or modification to an existing system may have on the personal privacy of the public or those who work for the Federal government. The PIA allows the DHA Privacy Office to determine if the new system is compliant with relevant data protection legislation and DoD policy requirements. The PIA also fosters transparency and openness to inform the public of what PII is collected, and how the government will use the PII.

For consistency, the program office or system owner should complete the DoD PIA template, DD Form 2930. Upon completion, e-mail the form without signatures to the DHA Privacy Office at dha.ncr.pcl.mbx.piamail@mail.mil.

Instructions

On page one of the PIA, enter the name of the DoD information system or electronic collection name, enter the DoD component's name that owns the system, which is the Defense Health Agency.

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).

If the answer is no, annotate in the DoD Information Technology Portfolio Repository (DITPR) or the authoritative database that updates DITPR as to why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, annotate in the appropriate documentation why a PIA is not required.

If the answer is yes, a PIA is required so proceed to Section 2.

Section 2: PIA Summary Information

a. Why is this PIA being created or updated?

You can only select one of the following: New information system; Existing DoD information system; System was significantly modified; New electronic collection; Existing electronic collection.

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

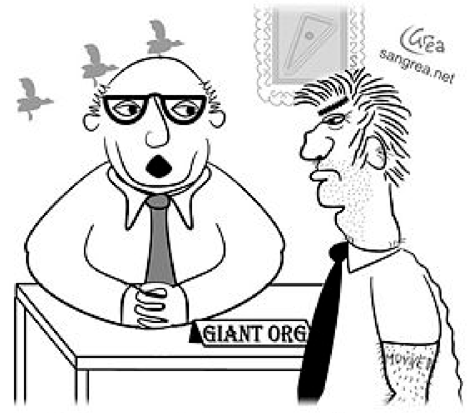
If the information system is registered in DITPR or SIPRNET, you need to add the DITPR or SIPRNET identification number. If you are not sure about the DITPR or SPIRNET, contact the System Program Manager.

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?

Requests the IT investment UPI (now called the Unique Investment Identifier (UII)) for the information system. If you do have the UII, type the UII in the block provided. If you do not have the UII, you can contact the DHA IT Budget Point of Contact to obtain the UII.

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. If the information system or collection system has a SORN, enter the Privacy Act SORN Identifier DoD Component-assigned designator, not the Federal Register number. Please reference the DHA Privacy Office website for current DHA SORNs.



Your DNA tests revealed that you are, in fact, a 93 year-old Chinese woman. I'm sorry, but since this job involves heavy lifting we cannot hire women or seniors.

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

Approval from the Office of Management and Budget (OMB) is required to collect data from 10 or more members of the public in a 12-month period regardless of form or format. If a form and/or information system is used to collect data from ***other than*** DoD military, DoD civilians, or other Federal employees, OMB approval is required unless there is an exemption noted in the approved authority. If you checked yes, please provide the OMB Control Number and expiration in the appropriate block. You can contact the DHA Information Management Control Officer (IMCO) or DoD Clearance Officer for this information.

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.

Provide the specific legal authorities (statutes or Executive orders), and policies for the DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. Some authorities may be found in the SORN identified for this system.

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) You will describe the purpose of the DoD information system or electronic collection and the types of personal information about individuals collected in the system. Explain the primary uses of the system showing how the information system will use the PII. Provide a general description of personal information about individuals that is collected in the information system (e.g. personal descriptors, ID numbers, ethnicity, health, financial, employment, credit); categories of individuals (e.g. dependents, retirees and/or their dependents, active duty, contractors, foreign nationals, former spouses, reservist, national guard personnel) that information will be collected from (or about) within the system. In this section, provide the name of the office that owns and/or manages the information system. Please do not include actual PII as this section will be published on the DHA Privacy Office website.

(2) You will describe the privacy risks associated with the PII collected and your mitigation strategy to reduce the risks. Response should indicate how you have identified and mitigated any privacy risks in the system / application (e.g., awareness and training programs, limited physical access, data encryption, violations for unauthorized monitoring, etc.) in order to sufficiently reduce system / application vulnerabilities to a reasonable and appropriate level. (Note: it is appropriate to address administrative, physical, and technical controls in place to protect the system (DoDI 8580.02, Security of Individually Identifiable Health Information in DoD Health Care Programs, Enclosure 4).)

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)?

If your system / application shares data with another system / application, include that system under the appropriate sub-category listed below. Please provide a short explanation of why this PII is shared. If you do not know whether systems share data, you can contact the business owner of the data or the IT specialist who knows what other interfaces exists between the systems / applications. For information shared with contractor(s), please indicate whether Business Associate Agreement or other appropriate privacy contract language is provided in the contract(s) (if applicable).

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

The opportunity to object is only available at the initial point of data collection. If your system receives PII from a system-to-system interface, the opportunity to object is only available at the source system. You will explain the method(s) individuals can use to object to each mode of collection (e.g., telephone, face-to-face, etc.). You will also explain the consequences, if any, if an individual objects (i.e., comprehensive healthcare may not be possible).

DoD 5400.11-R, Department of Defense Privacy Program, C4, Disclosures of Personal Information to Other Agencies and Third Parties, lists the approved circumstances wherein an individual would not be given an opportunity to object to the collection of their PII.

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

Explain how consent is obtained from individuals after they provide their PII. If applicable, explain how authorization is obtained from individuals after they provide their PHI. You also need to explain if consent requires a positive action by an individual rather than being assumed as a default. Explain the positive action if one is required.

Explain if the refusal of an individual to consent to the collection or use of personal information disrupts the level of program service provided to the individual (e.g., comprehensive healthcare may not be possible). Include the method(s) individuals can use to consent to each specific use (e.g., telephone, face-to-face, etc.) of PII. Include consequences, if any, if an individual withholds consent (e.g., comprehensive healthcare may not be possible).

k. What information is provided to an individual when asked to provide PII data?

According to DoD 5400.11-R, C2.1.4., when an individual is requested to furnish PII, a Privacy Act Statement is required, regardless of medium (e.g., telephone, form, personal interview). When an individual is requested to furnish personal information about him or her for inclusion in a system of records, a Privacy Act Statement is required to enable the individual to make an informed decision whether to provide the information requested. If PII is solicited by a DoD system (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. You will be required to insert the Privacy Act Statement or the Privacy Advisory.

In compliance with Section 208 of the E-Government Act of 2002, Sections 1 and 2 are posted 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 3: PIA Questionnaire and Risk Review

a. For questions in subparagraphs 3.a.(1) through 3.a.(5), indicate what PII (a data element alone or in combination that can uniquely identify an individual) will be collected and describe the source, collection method, purpose, and intended use of the PII.

(1) What PII will be collected?

Identify and list individual PII or PII groupings that is collected and stored in the system. This could include, but is not limited to, name, other names used, birth date, citizenship, legal status, mailing/home address, telephone number, social security number (SSN), truncated SSN, personal e-mail address, mother's maiden name, race/ethnicity, medical information, financial information, medical information, marital status, spouse information, child information, biometrics, disability information, driver's license, place of birth, or any other PII. If you select "other", please specify what information is being collected.

(2) What is the source for the PII collected (e.g., individual, existing DoD information systems, other Federal information systems or databases, commercial systems)?

List existing DoD information systems, other Federal information systems or databases, or commercial systems that provide the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources, such as commercial data aggregators?

(3) How will the information be collected?

Describe why information from sources other than the individual are required. For example, if a program is using data from a commercial aggregator of information, state the fact that this is where the information is coming from and explain why the program is using this source of data.

Provide form number(s) and name(s) if form(s) are used to collect PII. Also, provide URL if PII is collected via web site.

(4) Why are you collecting the PII selected (e.g., verification, identification, authentication, data matching)?

Please include the PII category and reason it is being used. Merely stating the general purpose of the system without explaining why particular types of personally identifiable information should be collected and stored is not an adequate response to this question.

(5) What is the intended use of the PII collected (e.g., mission-related use, administrative use)?

Provide a statement explaining how this PARTICULAR personally identifiable information that is collected and stored in the system is necessary to the component's or to the DHA's mission.

b. Does this DoD information system or electronic collection create or derive new PII about individuals through data aggregation? (See Appendix II for data aggregation definition.)

If "Yes," explain what risks are introduced by this data aggregation and how risk is mitigated.

Response should indicate:

- If the system creates or makes available new or previously unavailable information about an individual; and
- What will be done with the newly identified derived information?

Are (or will there be) computer data matching agreement(s) in place which describe who will be responsible for protecting the privacy rights of the beneficiaries and employees affected by the interface between the systems?

c. Who has or will have access to PII in this DoD information system or electronic collection?

Identify and list the types of users. For example, managers, system administrators, contractors, and developers may have access to the system. Identify users from other agencies that may have access to the system and under what roles do these individuals have access to the system. Also, describe the level of access for each role.

d. How will the PII be secured?
(1) Physical Controls.

In addition to the selected options, address if the system currently or will be accessed at more than one site. If the system is operated in more than one site, explain how consistent use of the system and data will be maintained at all sites.

(2) Technical Controls.

In addition to the selected options, explain if the data is encrypted in transit and/or at rest. Address if the system hosts or will host a web site accessible by the public.

(3) Administrative Controls.

In addition to the selected options, explain where backups occur, how often they occur, and how the data is safeguarded. If backups are not encrypted, please provide the DHA Privacy Office with a Plan of Action & Milestones documenting when encryption will occur.

Address if the system has a user's manual, and maintain audit logs. Explain the current or future processes in place for periodic review of PII contained in the system to ensure data integrity, availability, accuracy, and relevancy. Additionally, address any training for users of the system.

e. Does this DoD information system require certification and accreditation under the DoD Information Assurance Certification and Accreditation Process (DIACAP)?

Please check the appropriate box and enter the date. If you have not received your certification or accreditation (C&A), please specify your expected date of completion below, next to the C&A currently being pursued and provide a status of the DIACAP in question g. or h. (whichever applies). This is also applicable to the risk management framework (RMF) process.

f. How do information handling practices at each stage of the "information life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individuals' privacy?

According to OMB Circular No. A-130, "the term 'information life cycle,' means the stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition." For the purposes of the PIA, the stages are collection, use, disclosure, processing, retention, and destruction.

Please address each information life cycle phase as listed below:

Collection – Explain how the system collects only the personal information necessary for its purposes. Will steps be taken to ensure that the personal information is accurate, complete, and up-to-date?
Use and Disclosure – Explain how the system ensures that the sharing of information is to only those identified in the SORN and how PII violations are handled.
Processing – Explain how data exchange will take place (e.g. over an encrypted network), how component systems and / or applications limit information sharing to those that are functionally necessary.
Retention and Destruction – Indicate which data retention and destruction schedule(s) are implemented. Explain what and how policies of individual component systems, as stated in their SORNs, govern the retention and disposal of PII collected.

Additionally, please indicate the current system life cycle phase from the following:

- Concept Refinement
- Technology Development
- System Development and Demonstration
- Production and Deployment
- Operations and Support
- Disposal or Decommissioning

g. For existing DoD information systems or electronic collections, what measures have been put in place to address identified privacy risks?

If your information system is a new system, enter N/A and skip to question h.

You must address the following in your answer / risk assessment:

- Is all PII evaluated for impact of loss or unauthorized disclosure and protected accordingly?
- Are all electronic PII records assigned a High or Moderate impact category and protected at a Confidentiality level of Sensitive or higher, unless specifically cleared for public release (Ref. Guide to Protecting the Confidentiality of Personally Identifiable Information" - Special Pub 800-122 or FIPS Pub 199 "Standards for Security Categorization of Federal Information and Information Systems")?
- [If applicable] Are High impact category PII records routinely processed or stored on mobile computing devices or removable electronic media?
- [If applicable] May High impact PII records be accessed by users remotely?
- If PII / PHI may be downloaded to a workstation, mobile computing device, or removable electronic media, what mechanisms are in place to secure that media from unauthorized disclosure, theft, or loss?
- [If applicable] May mobile computing devices that contain High impact PII, including those approved for routine processing, be removed from protected workplaces?
- [If applicable] Does the website employ (or will it employ) persistent tracking technology?
- Are employees or agents with access to personal information in your organization provided with training related to privacy protection?
- Are programs and information technology staff aware of the relevant policies regarding breaches of security or confidentiality?
- Are there controls in place to ensure that data is not made available or disclosed to unauthorized individuals, entities, or processes?
- Are there controls in place to ensure that data has not been altered or destroyed in an unauthorized manner?

h. For new DoD information systems or electronic collections, what measures are planned for implementation to address identified privacy risks?

You must address the following in your answer / risk assessment:

- Is all PII evaluated for impact of loss or unauthorized disclosure and protected accordingly?
- Are all electronic PII records assigned a High or Moderate impact category and protected at a Confidentiality level of Sensitive or higher, unless specifically cleared for public release (Ref. Guide to Protecting the Confidentiality of Personally Identifiable Information" - Special Pub 800-122 or FIPS Pub 199 "Standards for Security Categorization of Federal Information and Information Systems")?
- [If applicable] Are High impact category PII records routinely processed or stored on mobile computing devices or removable electronic media?
- [If applicable] May High impact PII records be accessed by users remotely?

- If PII / PHI may be downloaded to a workstation, mobile computing device, or removable electronic media, what mechanisms are in place to secure that media from unauthorized disclosure, theft, or loss?
- [If applicable] May mobile computing devices that contain High impact PII, including those approved for routine processing, be removed from protected workplaces?
- [If applicable] Does the website employ (or will it employ) persistent tracking technology?
- Are employees or agents with access to personal information in your organization provided with training related to privacy protection?
- Are programs and information technology staff aware of the relevant policies regarding breaches of security or confidentiality?
- Are there controls in place to ensure that data is not made available or disclosed to unauthorized individuals, entities, or processes?
- Are there controls in place to ensure that data has not been altered or destroyed in an unauthorized manner?

Section 4: Review and Approval Signatures

Provide a contact name, title, organization, telephone number, and e-mail address for the program manager of the system or program covered by the PIA. Do not sign the PIA until told to do so by DHA Privacy Office.

Appendix I
PIA Triggers

According to OMB Memorandum M-03-22, the system activities listed below may trigger a PIA:

Conversions - when converting paper-based records to electronic systems;

Anonymous to Non-Anonymous - when functions applied to an existing information collection change anonymous information into information in identifiable form;

Significant System Management Changes - when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system: For example, when an agency employs new relational database technologies or web-based processing to access multiple data stores, such additions could create a more open environment and avenues for exposure of data that previously did not exist.

Significant Merging - when agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated. For example, when databases are merged to create one central source of information, such a link may aggregate data in ways that create privacy concerns not previously at issue.

New Public Access - when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public;

Commercial Sources - when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources. (Merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement);

New Interagency Uses - when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government initiatives; in such cases, the lead agency should prepare the PIA;

Internal Flow or Collection - when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form; and

Alteration in Character of Data - when new information in identifiable form added to a collection raises the risks to personal privacy. For example, the addition of health or financial information may lead to additional privacy concerns that otherwise would not arise.

Appendix II
Definitions

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 of Information. 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.

Note: If the system collects data from 10 or more members of the public (see federal personnel definition in the appendix) in a 12-month period, there is a requirement for an OMB Control Number (unless there is an exemption noted in an approved authority).

National Security Systems. As defined in the Clinger-Cohen Act, an information system operated by the federal government, the function, operation or use of which involves: (a) intelligence activities, (b) cryptologic activities related to national security, (c) command and control of military forces, (d) equipment that is an integral part of a weapon or weapons systems, or (e) systems critical to the direct fulfillment of military or intelligence missions, but does not include systems used for routine administrative and business applications, such as payroll, finance, logistics and personnel management.

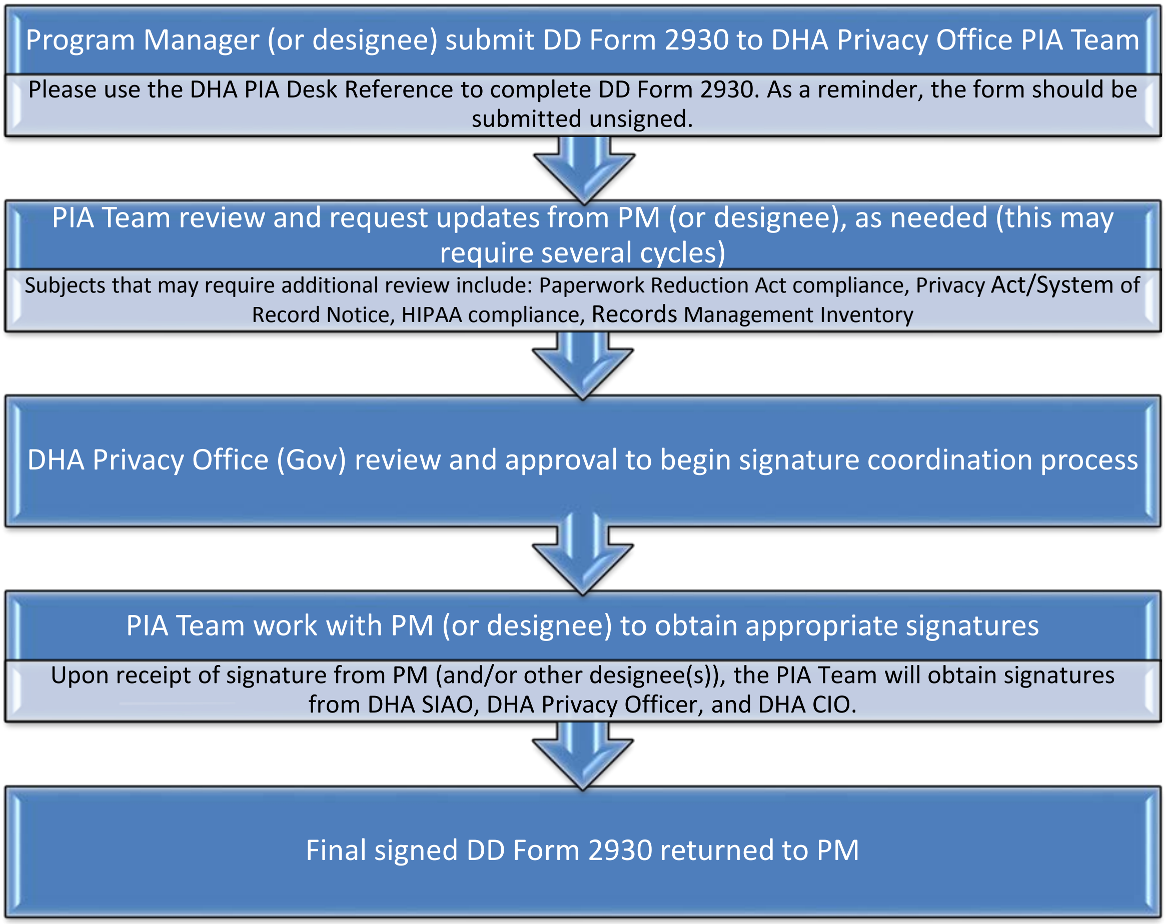
Personally Identifiable Information. Information about an individual that identifies, links, relates or is unique to, or describes him or her (e.g., a social security number; age; marital status; race; salary; home telephone number; other demographic, biometric, personnel, medical, and financial information). 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 system (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.

System of Records Notice (SORN). Public notice of the existence and character of a group of records under the control of an 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 include.

Appendix III
PIA Process



Program Manager (or designee) submit DD Form 2930 to DHA Privacy Office PIA Team

Please use the DHA PIA Desk Reference to complete DD Form 2930. As a reminder, the form should be submitted unsigned.

PIA Team review and request updates from PM (or designee), as needed (this may require several cycles)

Subjects that may require additional review include: Paperwork Reduction Act compliance, Privacy Act/System of Record Notice, HIPAA compliance, Records Management Inventory

DHA Privacy Office (Gov) review and approval to begin signature coordination process

PIA Team work with PM (or designee) to obtain appropriate signatures

Upon receipt of signature from PM (and/or other designee(s)), the PIA Team will obtain signatures from DHA SIAO, DHA Privacy Officer, and DHA CIO.

Final signed DD Form 2930 returned to PM

DHA Privacy and Civil Liberties Staff

Linda S. Thomas, JD, CIPP/G, PMP, CISSP
Chief, DHA Privacy and Civil Liberties Office
Chief, Freedom of Information Act
linda.s.thomas47.civ.mail.mil

Nadine Brown
Freedom of Information Act Officer
nadine.r.brown4.civ@mail.mil

Rita Deshields
Data Sharing Compliance Manager
rita.s.deshields.civ@mail.mil

John Eckert, Captain, USPHS
Human Research Protection
john.j.eckert14.mil@mail.mil

Rahwa Keleta
HIPAA Compliance Manager
rahwa.a.keleta.civ@mail.mil

Jennifer Noble, PhDc, MBA/HRM, FAHM, CIPP/G
Federal Privacy Compliance Manager
marilynn.j.noble.civ@mail.mil