BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-332

16 MAY 2011

Communications and Information

AIR FORCE PRIVACY PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at **www.e-publishing.af.mil** for downloading.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: SAF/A6PPF

Certified by: SAF/A6P
(Mr. Bobby Smart)

Supersedes: AFI 33-332, January 29, 2004

Pages: 58

This Instruction implements Air Force Policy Directive (AFPD) 33-3, *Information Management*; DoD 5400.11-R, *Department of Defense Privacy Program*; and DoD Instruction 5400.16, *DoD Privacy Impact Assessment (PIA) Guidance*; and is consistent with guidance in AFI 33-200, *Information Assurance Management*. It provides guidance for collecting, safeguarding, maintaining, using, accessing, amending and disseminating personally identifiable information (PII) in Air Force Privacy Act and other records whether in paper or electronic format. In general, as provided in DoD 6025.18R, *DoD Health Information Privacy Program*, protected health information is covered by the Privacy Act of 1974, 5 U.S.C. § 552a, DoD 5400.11-R, and this Instruction.

This Instruction applies to all Air Force active military and civilians, contractor employees in the performance of their duties to an Air Force contract, the Air Force Reserve, Air National Guard, and Civil Air Patrol when performing functions for the Air Force, and, IAW DoD 5100.3, *Support of the Headquarters of Combatant and Subordinate Joint Commands*. It also applies where the Air Force is the executive agent.

Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 33-363, Management of Records, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at **https://www.my.af.mil/afrims/afrims/afrims/rims.cfm**.

Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route through the appropriate functional's chain of command. Send supplements and implementing

publications of this Instruction, Chief of Warfighting Integration and Chief Information Officer (SAF/CIO A6), 1800 Air Force Pentagon, Washington DC 20330-1800 for review and coordination prior to publication.

This Instruction requires collecting and maintaining information protected by the *Privacy Act of 1974*, System of Records Notices (SORN) F033 AF B, *Privacy Act Request File*, and F036 AF PC Q, *Personnel Data Systems (PDS)* apply.

SUMMARY OF CHANGES

This Instruction has been substantially changed and must be completely reviewed. Major changes include: the Air Force Privacy Program structure, roles and responsibilities for Privacy Act Officer including designation of a Wing Privacy Officer; implements use of DD Form 2930, *Privacy Impact Assessment* (PIA) and guidance for completion; implements 120 day timeline for completion of PIA; clarifies guidance when PIA is not required for an IT system; implements PIA and SORN review frequency to coincide with annual Federal Information System Management Act (FISMA) reviews; implements DoD Social Security Number (SSN) Reduction Plan guidance for both paper and electronic systems of records and AF forms; implements OSD guidance for Safeguarding Against and Responding to Breach of Personally Identifiable Information (PII) and PII Incident Reporting and Risk Assessment Model; includes guidance for appointment of PII Incident Inquiry Officer; implements specialized Privacy Act training for those whose job duties require handling PII and signing annual certification of Privacy Act training after completion of Total Force Air Force Training (TFAT); implements DoD Privacy Office quarterly reporting of Privacy Act Training activities and Section 803 - 9/11 Commission activities; clarifies use of FOUO; includes guidance for DoD PKI encryption of emails containing Privacy Act information; clarifies the response timeline of 10 days for Privacy Act record requests; clarifies when a SORN is required (when record is retrieved by name or personal identifier); implements 120 days timeline for completion of SORN; clarifies SORN 30 days public comment period; prohibits the storage of PII on SharePoint unless required for daily business and or mission requirements; implements the requirement for a PIA to be completed whenever storing of PII on SharePoint for daily business or mission requirements; implements requirements for storing PII in electronic files or folders.

Chapter 1

OVERVIEW OF THE PRIVACY PROGRAM

1.1. Basic Guidelines.

1.1.1. Records that are retrieved by name or other personal identifier of a U.S. citizen or alien lawfully admitted for permanent residence are subject to Privacy Act requirements and are referred to as a Privacy Act system of records. The Air Force must publish SORNs in the *Federal Register*, describing the collection of information for new, changed or deleted systems to inform the public and give them a 30 day opportunity to comment ***before*** implementing or changing the system. (See Attachment **2**).

1.1.1.1. In the Privacy process, The Privacy Act of 1974 defines the term "record" as 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 name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

1.1.1.2. In the Records Management process, 44 U.S.C., Section 3301 defines the term "records" as all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, guidance, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them." Records Management has a broader definition of "record" than the Privacy Act definition.

1.1.2. An official Privacy Act system of records is:

1.1.2.1. Authorized by law or Executive Order or regulation; and

1.1.2.2. Necessary to carry out an Air Force mission or function; and

1.1.2.3. Published in the *Federal Register.*

1.1.3. The Air Force *shall not*:

1.1.3.1. Keep records on how a person exercises First Amendment rights. First Amendment rights include, but are not limited to, freedom of religion, freedom of political beliefs, freedom of speech, freedom of the press, the right to assemble, and the right to petition. *EXCEPTIONS are when:* The Air Force has the permission of that individual or is authorized by Federal statute; or the information pertains to and is within the scope of an authorized law enforcement activity.

1.1.3.2. Penalize or harass an individual for exercising rights guaranteed under the Privacy Act.

1.1.4. Air Force members *shall:*

1.1.4.1. Keep paper and electronic records that are retrieved by name or personal identifier only in approved Privacy Act systems of records which have notices published in the *Federal Register*.

1.1.4.2. Collect, maintain, and use information in such systems ONLY for purposes described in the published system of records notice to support programs authorized by law, executive order, regulation, or policy.

1.1.4.3. Safeguard the records in the system, keep them the minimum time required, and dispose of them according to disposition instructions.

1.1.4.4. Ensure records are timely, accurate, complete, and relevant.

1.1.4.5. Amend and correct information in Privacy Act records upon request, as appropriate.

1.1.4.6. Allow individuals to review and receive copies of their own Privacy Act records unless an exemption for the system of records has been published in the *Federal Register*.

1.1.4.7. Provide a review of decisions that deny individuals access to or amendment of their information contained in Air Force Privacy Act records.

1.1.4.8. Ensure all electronic files or folders which contain PII have the proper restrictions to a "Need to Know" requirement to conduct daily official business.

1.1.4.9. Minimize the storage of PII on Shared Drives.

1.1.4.10. Ensure PII is not stored on SharePoint unless required for daily business or mission requirements.

1.1.4.11. Ensure a PIA is completed whenever PII is stored on SharePoint for business or mission requirements. (see Chapter **7**)

1.1.5. Penalties for Violation. An individual may file a civil law suit against the Air Force for failing to comply with the Privacy Act. In addition to specific remedial actions, civil remedies include payment of damages, court costs, and attorney fees in some cases. Any official or individual may also be found guilty of a misdemeanor and fined not more than $5,000 if they willfully:

1.1.5.1. Maintain a system of records without publishing the required public notice in the *Federal Register*; or

1.1.5.2. Disclose Privacy Act information from a system of records, knowing that dissemination is prohibited, to anyone not entitled to receive the information; or

1.1.5.3. Request or obtain access to Privacy Act information on another individual under false pretenses.

1.1.6. Privacy Act Complaints. Privacy Act complaints or allegations of Privacy Act violations are not the same as PII - Breaches (see Chapter **9**), Freedom of Information Act requests, or Privacy Act access requests. A Privacy Act complaint must be submitted in written form and is categorized and reported quarterly as follows (see Quarterly Reporting):

1.1.6.1. Process and Procedural: Consent, Collection, and Appropriate Notice.

1.1.6.2. Redress: non-Privacy Act inquiries seeking resolution of difficulties or concerns about Privacy matters.

1.1.6.3. Operational: Inquiries regarding Privacy Act matters not including Privacy Act requests for access and/or correction.

1.1.6.4. Referrals: Complaints received but referred to another office with jurisdiction over the complaint.

1.1.6.5. Complaints of Privacy Act violations are processed through the appropriate Privacy Act office. The Privacy Act officer directs the process and provides guidance to the system of records manager. In cases where no system of records manager can be identified, the local Privacy Act officer will assume the privacy complaint duties. Issues that cannot be resolved at the local level will be elevated to the HAF/MAJCOM/FOA/ or DRU Privacy Office, as appropriate.

1.1.6.5.1. The local system of records manager will:

1.1.6.5.1.1. Investigate complaints, or allegations of Privacy Act violations.

1.1.6.5.1.2. Establish and review the facts when possible.

1.1.6.5.1.3. Interview individuals as needed.

1.1.6.5.1.4. Determine validity of the complaint.

1.1.6.5.1.5. Make appropriate corrective actions.

1.1.6.5.1.6. Ensure a response is sent to the complainant through the Privacy Act Officer.

1.1.6.5.1.7. When appropriate refer cases for more formal investigation, refer cases for command disciplinary action, and consult the servicing Staff Judge Advocate.

1.1.6.6. Unified combatant commands process component unique Privacy Act complaints through the respective component chain of command.

1.1.6.7. For Privacy Act complaints filed in a U.S. District Court against the Air Force, an Air Force activity, or any Air Force employee, AFLOA/JACL will provide SAF/A6P a litigation summary in accordance with the format in Appendix 8 of DoD 5400.11-R. When the court renders a formal opinion or judgment, AFLOA/JACL sends SAF/A6P a copy of the judgment and opinion.

1.1.7. Personal Notes. Do not file personal notes in a Privacy Act record, as personal notes if filed in a system of records retrieved by an individual's name or other personal identifier might be considered part of the Privacy Act record.

1.1.8. Systems of Records Operated by a Contractor. Contractors who by contract are required to operate or maintain a Privacy Act system of records must follow this Instruction. Such a Privacy Act system of record is considered to be maintained by the Air Force and is subject to this Instruction. System managers for offices who have contractors operating or maintaining Privacy Act system of records must identify the record system number and coordinate with the government manager of the contract to ensure the contract contains the proper Privacy Act clauses, and as required by the Defense Acquisition Regulation and this

Instruction. (See Federal Acquisition Regulation (FAR): **https://www.acquisition.gov/far/current/pdf/FAR.pdf** , *Privacy Act Notification:* 52.224-1 and *Privacy Act and the Defense FAR*: 52.224-2, Subpart 224.1., *Protection of Individual Privacy*).

1.1.8.1. Contracts for systems of records operated or maintained by a contractor will be reviewed annually by the appropriate HAF/MAJCOM/FOA/DRU Privacy Officer to ensure compliance with this Instruction.

1.1.8.2. Disclosure of Privacy Act records to a contractor for use in the performance of an Air Force contract is considered an official use disclosure within the agency under exception (b)(1) of the Privacy Act.

1.1.9. Responsibilities.

1.1.9.1. The SAF/CIO A6 shall appoint:

1.1.9.1.1. A Senior Agency Official for Privacy (SAOP) with overall responsibility for the Air Force Privacy Program

1.1.9.1.2. An Air Force Privacy Act Officer

1.1.9.2. The SAOP or the Air Force Privacy Act Officer serves as the Air Force member on the Defense Privacy Board and the Defense Data Integrity Board (DDIB) which are administered through the DoD Privacy Office (DPO).

1.1.9.3. The appellate authority, Deputy General Counsel (Fiscal, Ethics and Administrative Law) to the Secretary of the Air Force (SAF/GCA) makes final decisions on Privacy Act appeals. The General Litigation Division, AFLOA/JACL, receives Privacy Act appeals and provides recommendations to the appellate authority. Service unique appeals, from unified combatant commands, should go through the respective service component chain of command.

1.1.9.4. AF/JAA at Headquarters Air Force and Judge Advocate legal offices provide advice to Privacy officers, commanders, and supervisors on requests for Privacy Act records under the Privacy and Freedom of Information Act.

1.1.9.5. The Air Force Privacy Act Officer:

1.1.9.5.1. Administers guidance and procedures prescribed in this Instruction.

1.1.9.5.2. Provides guidance and assistance in implementation and execution of the Air Force Privacy Program to HAF/MAJCOM/FOA/DRU.

1.1.9.5.3. Conducts mandatory reviews of publications and forms for compliance with this Instruction.

1.1.9.5.4. Reviews and recommends Privacy Impact Assessments (PIA) to SAF/CIO A6 for approval. (See Chapter **7**)

1.1.9.5.5. Reviews and approves proposed new, altered, amended and deleted systems of records notices (SORNs).

1.1.9.5.6. Tracks and forwards PII Incident Reports from all AF sources to DPO within timelines and follows incident trends to improve guidance. (See Chapter **9**)

1.1.9.5.7. Ensures training and training tools are available for a variety of AF audiences. (See Chapter **11**)

1.1.9.5.8. Provides guidance and support to commands to ensure that information systems which are developed to collect, maintain, process, or disseminate Privacy Act data conform to Privacy Act requirements IAW this Instruction.

1.1.9.5.9. Coordinates with SAF/A6OI Information Assurance Division which ensures appropriate Information Assurance Control procedures and data safeguards are tested, implemented and maintained in IT systems by Information System Owners (ISO), Program Managers (PM), Information Assurance Managers (IAM), and Portfolio Managers during the Certification and Accreditation Process and to protect the Privacy Act information throughout the IT system life cycle.

1.1.9.6. AF Departmental Forms Management Officer: Maintains a database of both new and existing forms reviewed to produce an annual report every July 1. This report shall be submitted to the AF Privacy Officer as input into the Privacy section of the annual FISMA Report as required by subchapter III, chapter 35 of title 44, United States Code. (See paragraph **2.3** Social Security Number Reduction) Ensures OPRs for new and revised departmental forms that are collecting PII coordinate with the AF Privacy Act Officer before publishing. Final publishing packages must contain a completed DD Form 67, *Form Processing Action Request*, or AF Form 673, *Air Force Publication/Form Action Request*, (whichever is applicable IAW AFI 33-360, *Publications and Forms Management*) and copies of the Defense Privacy Official approved SSN justification memo and SORN. (see paragraph **2.3.2.1.2.2**).

1.1.9.7. MAJCOM/FOA/DRU commanders and HAF/IM implement this Instruction. Certain officials or a designee may deny access or amendment of records as authorized by the Privacy Act. (See paragraph **3.6** Denial Authorities**)**

1.1.9.7.1. HAF/IM will provide comprehensive Privacy Act support, training, and reporting for all HAF organizations.

1.1.9.7.2. Establish a Privacy Office and appoint a command Privacy Act Officer.

1.1.9.7.3. Direct the establishment of HAF/MAJCOM/FOA/DRU Privacy Offices and authorize appointment of HAF/MAJCOM/FOA/DRU Privacy Act Officer and organization Privacy Act Monitors to assist with implementation of this Instruction.

1.1.9.7.4. Direct local senior-level individuals in the chain of command for the organization where a PII Breach occurs to conduct an inquiry to gathers facts to determine if there was malicious intent which warrant a criminal investigation; take appropriate corrective and/or disciplinary actions, and make appropriate notifications to affected individuals in coordination with the HAF/MAJCOM/FOA/DRU privacy officials. (See paragraph **9.3** PII Breach Reporting)

1.1.9.7.5. Ensure coordination and teamwork is accomplished between system PM, IAMs and Privacy Officials.

1.1.9.8. HAF/MAJCOM/FOA/DRU Privacy Act Officers:

1.1.9.8.1. Provide quarterly updates of Privacy Officials' names, office symbols, voice number, FAX number, unclassified and/or classified email addresses to the Air Force Privacy Office (SAF/A6PPF) for POC continuity.

1.1.9.8.2. Ensure appropriate users receive annual specialized training and Privacy Act Systems of Record Training in addition to Privacy Act Annual Refresher Training.

1.1.9.8.3. Promote Privacy Act awareness throughout the HAF/MAJCOM/FOA/DRU and organizations.

1.1.9.8.4. Review subordinate publications and forms for compliance with this Instruction.

1.1.9.8.5. Resolve PII breaches by ensuring all actions are completed by the Privacy officers/Monitors to include notifications to individuals as required, and submit final PII Incident Reports to AF Privacy Office.

1.1.9.8.6. Submit Quarterly Training reports, FISMA reports, Section 803 and other reports as required and directed by the AF Privacy Office.

1.1.9.8.7. Review SORNs and PIAs annually to coincide with the IT system review cycle for Certification and Accreditation (C&A) and FISMA reviews. Coordination and teamwork is required between system PM, IAM and Privacy Official. (DoDI 5400.16)

1.1.9.8.8. Conduct Staff Assistance Visits (SAVs) as deemed necessary to ensure the health of the Air Force Privacy program. Evaluate the health of the privacy program annually by using checklists and other tools based on this Instruction as guidance.

1.1.9.8.9. Provide consultation to system PM and IAM for completing SORN and PIA on IT systems.

1.1.9.8.10. Resolve complaints or allegations of Privacy Act violations that cannot be resolved by the Base/Wing Privacy Monitors.

1.1.9.8.11. Review and process Privacy Act Request denial recommendations. (See paragraph **3.6** Denial Authorities**)**

1.1.9.8.12. Provide guidance as needed to subordinate units implementing this Instruction.

1.1.9.9. Information System Owners, Program Managers and Information Assurance Managers:

1.1.9.9.1. Implement Privacy processes and complete PIAs and SORNs as required by this Instruction. Coordination and teamwork is required between system PMs, IAMs and Privacy Officials. (DoDI 5400.16)

1.1.9.9.2. Determine early in the design phase of IT systems development what personal information will be collected, used, processed, stored, or disseminated in electronic Privacy Act systems of records.

1.1.9.9.3. Formulate Privacy Act requirements in early stages of information systems design, development, and data management to plan for and implement appropriate IA controls to safeguard PII.

1.1.9.9.4. Ensure Privacy Act records and other records containing PII are safeguarded or removed as required from all IT systems prior to disposal, replacement, or reuse of IT hardware storage components, i.e., hard disk drives.

1.1.9.9.5. PM reviews the SORN for their information systems concurrently with the FISMA annual review to validate if changes to the SORN are needed.

1.1.9.9.6. A PM whose system of records is an IT system registered in the Enterprise Information Technology Data Repository (EITDR) shall address and update responses to privacy questions in EITDR. Failure to do so may risk system non-concurrence by AF Privacy Officer during annual compliance review, certification, decertification, or request for funding.

1.1.9.10. Individuals whose jobs require routine work with and/or access to Privacy Act Records, and other records containing PII, are responsible to:

1.1.9.10.1. Complete specialized Privacy Act training annually to comply with paragraph **11.1.2.2,** in addition to Privacy Act Annual Refresher Training.

1.1.9.10.2. Immediately report any suspected or confirmed breaches of PII to the United States Computer Emergency Readiness Team (USCERT) within one hour of the discovery then to the local Privacy Act Monitor or Officer, in accordance with the procedures outlined in Chapter **9**.

1.1.9.11. All other personnel subject to this Instruction are responsible to:

1.1.9.11.1. Safeguard and protect Privacy Act Records and PII contained in other Air Force records IAW this Instruction.

1.1.9.11.2. Immediately report any suspected or confirmed breaches of Privacy Act Records, and other records containing PII, to the local Privacy Act Officer or Monitor to comply with Chapter **9**.

Chapter 2

COLLECTING PERSONAL INFORMATION FROM INDIVIDUALS

2.1. Each agency that maintains a system of records shall:

2.1.1. Maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute, executive order or their implementing regulations;

2.1.2. Collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs;

2.1.3. Inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual. This is otherwise known as a Privacy Act Statement (PAS). A PAS may be provided verbally or in writing. A sign may also be displayed with the PAS in the area where the information is routinely requested;

2.1.3.1. Authority: the legal authority that authorizes the solicitation of the information and whether the disclosure of such information is mandatory or voluntary;

2.1.3.2. Purpose: the principal purpose or purposes for which the information is intended to be used;

2.1.3.3. Routine Uses: Who will have access to the information outside the DoD.

2.1.3.4. Disclosure: Voluntary or Mandatory. **(Use Mandatory only when disclosure is required by law and the individual will be penalized for not providing information; must have SJA review). Include any consequences of nondisclosure in nonthreatening language.**

2.1.4. Examples of when it is more practicable to collect information from a third party about another individual, instead of the subject individual, include:

2.1.4.1. Verification of information through third-party sources for security or employment suitability determinations;

2.1.4.2. Seeking third-party opinions such as supervisor comments as to job knowledge, duty performance, or other opinion-type evaluations;

2.1.4.3. When obtaining information first from the individual may impede rather than advance an investigative inquiry into the actions of the individual.

2.1.4.4. Contacting a third party at the request of the individual to furnish certain information, such as exact periods of employment, termination dates, copies of records, or similar information;

2.1.4.5. Collecting information on minor children.

2.2. Privacy Act Notifications:

2.2.1. Privacy Advisory. A notification informing an individual as to why personal information is being solicited and how such information will be used for a non-Privacy Act

record. When the same information is solicited for a Privacy Act record, the notification is referred to as a PAS. If PII is solicited on 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.

2.2.2. Privacy Act Statement in Publications. Include a Privacy Act Advisory Statement in each Air Force publication that requires collecting or keeping personal information in a system of records. Also include a Statement when publications direct collection from the individual of any part or form of the SSN. The Statement will refer to the legal authority for collecting the information and SORN number and Title as follows:

2.2.2.1. "This publication requires the collection and or maintenance of information protected by the Privacy Act of 1974 authorized by [set forth the legal authority such as the federal statute, executive order, or regulation]. The applicable Privacy Act SORN(s) [*number and title*] is available at http://privacy.defense.gov/notices/usaf/

2.2.3. Paper documents and materials that contain personal information protected under the Privacy Act such as recall rosters, personnel rosters, lists or spreadsheets shall be marked in the header or top "FOR OFFICIAL USE ONLY" with the following banner in the footer or bottom:

2.2.3.1. "The information herein is For Official Use Only (FOUO) which must be protected under the Freedom of Information Act of 1966 and Privacy Act of 1974, as amended. Unauthorized disclosure or misuse of this PERSONAL INFORMATION may result in criminal and/or civil penalties"

2.2.3.2. Paper documents and printed materials that contain PII shall be covered with the AF Form 3227 or DD Form 2923, Mar 2009, Privacy Act Cover Sheet (see paragraph **9.4.3**) when removed from a system of records.

2.2.4. The Privacy Act requires agencies to provide safeguards to ensure the security and confidentiality of Privacy Act records and to protect individuals against an invasion of personal privacy. Refer to AFI 33-129, *Transmission of Information Via the Internet*, for the appropriate procedures required to send Privacy Act information across the Internet.

2.2.4.1. Exercise caution before transmitting personal information over E-mail to ensure the message is adequately safeguarded. Some information may be so sensitive and personal that E-mail may not be the proper way to transmit it. When sending personal information over E-mail within DoD, ensure:

2.2.4.2. There is an official need.

2.2.4.3. All addressees (including "cc" addressees) are authorized to receive it under the Privacy Act.

2.2.4.4. It is protected from unauthorized disclosure, loss, or alteration.

2.2.5. E-mails shall be encrypted when they contain FOUO and Privacy Act Information sent to other Air Force or DoD offices for official purposes. Additional protection methods may include password protecting the information in a separate Microsoft Word™ document. When transmitting personal information over E-mail, add For Official Use Only ("FOUO") to the beginning of the subject line, followed by the subject, and apply the following

statement at the beginning of the e-mail: "The information herein is For Official Use Only (FOUO) which must be protected under the Privacy Act of 1974, as amended. Unauthorized disclosure or misuse of this PERSONAL INFORMATION may result in criminal and/or civil penalties." Do not indiscriminately apply this statement to E-mails. Use it only in situations when you are actually transmitting personal information for official purposes within the Government. See *DoD 5200.1-R Information Security Program*. Note: The guidance in this paragraph does not apply to appropriate releases of personal information to members of the public via e-mail, such as pursuant to the Freedom of Information Act, or with the consent of the subject of the personal information.

2.2.6. Do not send Privacy Act information to distribution lists or group e-mail addresses unless each member has an official need to know the personal information. Official e-mails messages will be digitally signed and encrypted (MGS). Before forwarding E-mails you have received that contain personal information, verify that your intended recipients are authorized to receive the information under The Privacy Act.

2.3. Social Security Number (SSN) Reduction. The stated intention of the Social Security Reduction Plan is to reduce or eliminate the use of SSN in DoD and AF systems of records, IT systems and forms. The Office of Primary Responsibility (OPR) for SSN Reduction shall be the data owner of systems of records, IT systems and AF forms with assistance from the Records Professional, the Privacy Official, and Forms Manager. The use of the SSN shall be limited to transactions that specifically require the presentation of the SSN to meet a statutory or regulatory requirement. Most applications that require the SSN for specific transactions do not require its use for every transaction. For example, systems that link to financial institutions may need the SSN for initial interactions, but thereafter use an account number or some other form of identification or authentication. As such there is no need to use the SSN for individuals to authenticate themselves as part of every transaction. Prior to the issuance of the DoD Instruction, the Directive Type Memorandum (DTM)-*07-015-USD (P&R), DoD Social Security Number (SSN) Reduction Plan*, 28 Mar 2008, **http://www.defenselink.mil/privacy/files/SSNReductionPlan.pdf** is in effect and establishes:

2.3.1. Acceptable Uses. Use of the SSN includes *the SSN in any form, including, but not limited to truncated, masked, partially masked, encrypted, or disguised SSN.* The acceptable uses of the SSN are those that are provided for by law, require interoperability with organizations beyond the Department of Defense, or are required by operational necessities. Such operational necessities may be the result of the inability to alter systems, processes, or forms due to cost or unacceptable levels of risk. Those systems, processes, or forms that claim "operational necessity" shall be closely scrutinized. Ease of use and unwillingness to change are not acceptable justifications for this case.

2.3.2. Documenting Acceptable Uses of PII and SSN specifically. The authorization for use of PII is governed through the DoD Privacy Program. The method by which SSN use is documented shall be consistent with existing Privacy program requirements for forms, processes, IT systems, and systems of records, to include any locally created applications.

2.3.2.1. In addition to the documentation required for the use of PII in the PIA and/or SORN, the use of the SSN in any form as part of any collection, transfer, or retention including locally created user applications must be specifically documented and justified.

Documentation for SSN justification shall be retained and available upon request. This documentation shall include:

2.3.2.1.1. The specific requirement for use of the SSN.

2.3.2.1.2. A senior official (flag officer or SES equivalent) shall sign a memorandum stating the justification for use of the SSN. It is unacceptable to collect, retain, use or transfer SSN without an approved justification.

2.3.2.1.2.1. Justification memo to collect SSN in an IT System shall be forwarded with the PIA and/or SORN to the AF Privacy Officer. The justification memo will be addressed to Defense Privacy Official for approval/disapproval. (See Attachment **6**).

2.3.2.1.2.2. Forms that collect SSN must have a completed DD Form 67 or AF Form 673, (whichever is applicable IAW AFI 33-360) and a justification memo (IAW paragraph 2.3.2.1.2.1) that is addressed to and approved by DoD Privacy Officer. Submit items to appropriate Forms Manager IAW AFI 33-360.

2.3.2.1.3. The Defense Privacy Officer reviews SSN justifications for IT systems as an adjunct to the biennial PII review process. Where a justification for SSN use is rejected, the action officer will prepare a plan, to include milestones and a timeline, for the elimination of SSN usage.

2.3.3. Periodic Review of SSN Use and Justification. SSN use and justification memo review is a responsibility under the biennial review process for all forms. IT systems justification memo shall be reviewed for this purpose in conjunction with the FISMA Annual review.

2.3.4. Requesting the Social Security Number (SSN). When requesting an individual's SSN always give a Privacy Act Statement when the SSN will be placed in a Privacy Act record, or otherwise provide a Privacy Advisory to the individual as to why their SSN is being collected, for what purpose it will be used, and whether disclosure is mandatory.

2.3.5. The Air Force requests an individual's SSN and provides the Privacy Act Statement required by law when anyone enters military service or becomes an Air Force civilian employee. Confirmation of Employment Eligibility is an acceptable use. The Air Force uses the SSN as a service or employment number to reference the individual's official records. When you ask an Air Force service member or employee for an SSN as identification in the context of this stated use to retrieve an official record, you do not have to restate this information.

2.3.5.1. Alternative Means of Identifying Records. When law, executive order, or regulation does not require disclosing the SSN or when the system of records was created after January 1, 1975, you may ask for the SSN, but the individual does not have to disclose it. If the individual refuses to respond, use alternative means of identifying records. Executive Order 9397, *Numbering System for Federal Accounts Relating to Individual Persons*, November 22, 1943, has been amended by Executive Order 13478, *Amendments to Executive Order 9397 Relating to Federal Agency Use of Social Security Numbers*, November 18, 2008, which emphasizes the need to protect PII. The mandatory requirement to collect SSNs has been deleted. Executive Orders 9397 (SSN), as amended

shall be referenced when cited in PAS, PIA and SORN whenever SSN is collected, used, stored, or disseminated for acceptable uses within AF IT systems, on AF Forms, or in other physical media systems of records. IT systems, AF Forms, and AF records OPRs should also consult *DTM-07-015-USD (P&R)*, paragraph 2, Acceptable Uses. Contact the OPR's organizational Privacy Office for assistance.

2.3.5.2. Protection of SSN. SSNs are personal and unique to each individual. *The SSN in any form, including, but not limited to truncated, masked, partially masked, encrypted, or disguised SSN will be Protected as High Impact PII and marked* FOR OFFICIAL USE ONLY (FOUO). Within DoD do not disclose another person's SSN without an official need to know. Outside DoD SSNs are not releasable without the person's consent or unless authorized under one of the twelve exceptions to the Privacy Act (see paragraph **10.4**).

2.3.6. Reporting Results of Social Security Number Reduction.

2.3.6.1. New Departmental Forms. AF Departmental Forms Management Officer shall maintain a database to produce an annual report every July 1st. This report shall be an input into the Privacy section of the annual FISMA Report as required by subchapter III, chapter 35 of title 44, United States Code. The annual report shall contain the following elements:

2.3.6.1.1. Number of forms reviewed.

2.3.6.1.2. Number of forms requesting SSNs.

2.3.6.1.3. Number of SSN justifications accepted and rejected.

2.3.6.1.4. Examples of forms where SSNs were not allowed.

2.3.6.1.5. Examples of SSN masking or truncation.

2.3.6.2. For new forms issued below departmental level (HAF/MAJCOM/FOA/DRU, Wing, etc), no database shall be required as set forth in paragraph 2.3.6.1., above, with the exception of annual reporting to the AF Departmental Forms Management Officer each July 1st with respect to information as to those forms in which SSNs were proposed to be collected but was determined not to be necessary.

2.3.6.3. Existing Departmental Forms. AF Departmental Forms Management Officer shall report annually on July 1st the results of AF Forms reviews and submit via report to the AF Privacy Officer for input into the Privacy section of the Annual FISMA Report. This report shall include the following elements:

2.3.6.3.1. Total number of forms in the database.

2.3.6.3.2. Number of forms reviewed.

2.3.6.3.3. Number of forms containing SSNs.

2.3.6.3.4. Number of forms where justifications were questioned.

2.3.6.3.5. Number of SSN justifications accepted and rejected.

2.3.6.3.6. Examples of forms where SSNs were not allowed.

2.3.6.3.7. Examples of SSN masking or truncation.

2.3.6.4. For existing forms issued below departmental level (HAF/MAJCOM/FOA/DRU, Wing, etc.), no reports are required at the command and installation levels, with the exception of sharing best practices of specific examples where SSNs were eliminated or better masked, or unless for metrics collection at the AF level.

Chapter 3

GIVING FIRST PARTY ACCESS TO THEIR PRIVACY ACT RECORDS

3.1. Making a Request for Access. For a non-official request for their Privacy Act record(s), first party requesters or their designated representatives shall submit a signed written request for a copy of their records. Requesters need not state why they want access to their records. Verify the identity of the requester to avoid unauthorized disclosures. How you verify identity will depend on the sensitivity of the requested records. Identity can be verified in a number of ways, to include visually, personal knowledge of the requester, a signed letter or request via telephone or email, a notarized statement, or an unsworn statement. An unsworn declaration or notarized statement should be obtained in the following format:

3.1.1. "I declare under penalty of perjury (if outside the United States, add "under the laws of the United States of America") that the foregoing is true and correct. Executed on (date) (Signature)."

3.2. Processing a Request for Access. Immediately consult the local Privacy Act Officer to assure timely response to the request. Consider a request from an individual for his or her own records in a system of records under both the Freedom of Information Act (FOIA) and the Privacy Act regardless of the Act cited. The requester does not need to cite either Act if the records requested are contained in a system of records. Process the request under whichever Act gives the most information. When necessary, tell the requester which Act was used and why.

3.2.1. Requesters must adequately describe the records they want. They do not have to name a system of records number, but they should at least name a type of record or functional area. For requests that ask for "all records about me," ask for more information and tell the person how to review the government-wide systems of records published in the *Federal Register* or at http://privacy.defense.gov/notices/.

3.2.2. Requesters will not use government equipment, supplies, stationery, postage, telephones, or official mail channels for making non-official requests for Privacy Act records. However, system managers may process such requests and tell requesters that using government resources to make non-official requests for Privacy Act records is not authorized.

3.2.3. Response to all Privacy Act requests shall be made within 20 workdays of receipt. The requester will be informed of the status of their request after 10 workdays have elapsed, informing them of the status of their request and providing an approximate completion date of no more than 20 workdays from the date of initial receipt of the request.

3.2.4. Show or give a copy of the record to the requester within 10 workdays of receiving the request unless the system has an exemption published in the *Federal Register* as a final rule. Give information in a form the requester can understand. If the system is exempt from disclosure under the Privacy Act, follow the procedures addressed in paragraph **3.5**

3.3. Fees. Provide the first 100 pages free, and charge only reproduction costs for the remainder. Copies cost $.15 per page; microfiche costs $.25 per fiche. Charge fees for all pages of subsequent requests when copies of the same records.

3.4. Do not charge fees:

3.4.1. For official purposes, such as to respond to the proposed denial of a right, privilege, or benefit; disciplinary action; or if the requestor can get the record without charge under procedures governed by DoD or AF regulation applicable to the record (for example medical records).

3.4.2. For search.

3.4.3. For reproducing a document for the convenience of the Air Force.

3.4.4. For reproducing a record so the requester can review it.

3.4.5. Fee waivers. Waive fees automatically if the direct cost of reproduction is less than $15, unless the individual is seeking an obvious extension or duplication of a previous request for which he or she was granted a waiver. Decisions to waive or reduce fees that exceed $15 are made on a case-by-case basis.

3.5. Denying or Limiting Access. When a Privacy Act record will not be released under the Privacy Act, the request must be processed under the FOIA. If any part of the record is denied under the FOIA, the procedures in DoD Regulation 5400.7/AFMAN 33-302 are followed. For Privacy Act denials not processed under the FOIA, send a copy of the request, the record copy, and why you recommend denying access (include the applicable exemption) to the denial authority through the legal office and the Privacy Act office. Judge Advocate (JA) offices will include a written legal opinion. The legal opinion will not merely state that the decision is "legally sufficient," but will provide factual details and an analysis of the law and applicable regulations. The Privacy Act officer reviews the file, and makes a recommendation to the denial authority. The denial authority sends the requester a letter with the decision. If the denial authority grants access, release the record copy. If the denial authority refuses access, tell the requester why and explain pertinent appeal rights (see Chapter **5**).

3.5.1. Before you deny a request for access to a record, make sure that:

3.5.1.1. The system has an exemption published in the *Federal Registe*r as a final rule.

3.5.1.2. The exemption covers each document. All parts of a system are not automatically exempt.

3.5.1.3. The FOIA does not require release of any part of the record.

3.5.1.4. Nonexempt parts are segregated.

3.5.2. Third Party Information in a Privacy Act System of Record. A first party requester is *not* entitled to information that is not "about" him or her that is contained in their Privacy Act record; for example, the home address or SSN of a third party. Servicing legal offices should be consulted prior to the release of a third party's sensitive personal information to a first party requester that is contained in the first party requester's Privacy Act record.

3.6. Denial Authorities.

3.6.1. Initial Denial Authority (IDA). An official who has been granted authority by the head of a DoD component to withhold records requested under the FOIA for one or more of the nine categories of records exempt from mandatory disclosure. See DoD 5400.7-R/AFMAN 33-302, *DoD Freedom of Information Act Program*. IDA's may also deny a fee category claim by a requester; deny a request for expedited processing due to demonstrated compelling need in accordance with DoD Regulation 5400.7/AFMAN 33-302*;* deny a

request for a waiver or reduction of fees; review a fee estimate; and confirm that no records were located in response to a request.

3.6.2. Only approved IDAs will deny all or parts of records. However, if the only information withheld from an Air Force record is privacy information under the DoD policy to withhold lists of names of DoD personnel ("DoD Names Policy"), the organization/unit FOIA monitors may sign the decision memorandum and FOIA managers may release on their behalf. FOIA managers may: initially deny fee category claims, requests for expedited processing, and waiver or reduction of fees; review fee estimates; and sign "no records" responses. IDAs are the deputy chiefs of staff and chiefs of comparable offices or higher at HQ USAF and Secretary of the Air Force (SAF) and MAJCOM commanders. MAJCOM commanders may appoint two additional positions at the headquarters and also the wing commander at base level. MAJCOM inspector general's (IGs) and MAJCOM Directors of Inquiries (IGQ) may act as IDAs for IG records. MAJCOM FOIA managers must notify SAF/A6PP in writing (by facsimile, e-mail, or regular mail) of IDA position titles. Send position titles only--no names. SAF/A6PP provides SAF/IGQ a courtesy copy of correspondence designating IDA positions for IG records. When the commander changes the IDA designee position, MAJCOM FOIA managers advise SAF/A6PP immediately. In the absence of the designated IDA, the individual filling/assuming that position acts as an IDA, however; all denial documentation must reflect the position title of the approved or designated IDA, even if in an acting capacity (i.e., Acting Director of Communications and Information, Headquarters Air Combat Command). Organizations are authorized to withhold DoD names below 0-7, and email addresses of most DoD personnel, under the DoD Names Policy.

3.6.3. HAF two-letter/digit offices.

3.6.4. MAJCOM/FOA/DRU commanders.

3.6.5. Unified Commanders.

Chapter 4

AMENDING A PRIVACY ACT RECORD

4.1. Amendment Reasons. Individuals may ask to have their personal information in records amended to make them accurate, timely, relevant, or complete. System managers will routinely correct a record if the requester can show that it is factually wrong (e.g., date of birth is wrong).

4.2. Responding to Amendment Requests.

4.2.1. The individual may request simple corrections orally. Requests for complicated and detailed corrections must be in writing to ensure clarity.

4.2.2. After verifying the identity of the requester, make the change if appropriate, notify all known recipients of the record, and inform the individual.

4.2.3. Acknowledge requests within 10 workdays of receipt. Give an expected completion date unless you complete the change within that time. Final decisions must, unless extended by the appropriate authority, take no longer than 30 workdays.

4.3. Approving or Denying a Record Amendment. The Air Force does not usually amend a record when the change is based on opinion, interpretation, or subjective official judgment. Determination not to amend such records constitutes a denial, and requesters may appeal (see Chapter **5**).

4.3.1. If the system manager decides not to amend the record, send a copy of the request, the record, and the recommended denial reasons to the denial authority through the legal office and the Privacy Act office. Legal offices will include a written legal opinion. The legal opinion will not merely state that the decision is "legally sufficient," but will provide factual details and an analysis of the law and applicable regulations. The Privacy Act officer reviews the proposed denial and legal opinion and makes a recommendation to the denial authority.

4.3.2. The denial authority sends the requester a letter with the decision. If the denial authority approves the request the record is amended.

4.3.3. The requester may file a concise statement of disagreement with the system of records manager if SAF/GCA denies the request to amend the record. SAF/GCA explains the requester's rights when they issue the final appeal decision. (see Privacy Act of 1974)

4.4. Contents of Privacy Act Processing Case Files. Do not keep copies of disputed records in this file. File disputed records in their appropriate series. Use the file solely for statistics and to process requests. Do not use the case files to make any kind of determination about an individual. Document the reasons for untimely responses. These files include:

4.4.1. Requests from and replies to individuals on whether a system has records about them.

4.4.2. Requests for access or amendment.

4.4.3. Approvals, denials, appeals, and final review actions.

4.4.4. Coordination actions and related papers.

Chapter 5

APPEALS

5.1. Appeal Procedures. Individuals who receive a denial to their access or amendment request may request a denial review (appeal) within 60 calendar days of the date of the denial letter. (See paragraph 3.6. Denial Authorities)

5.1.1. The denial authority promptly sends a complete appeal package to SAF/GCA. The package must include:

5.1.1.1. The original appeal letter;

5.1.1.2. The initial request;

5.1.1.3. The initial denial;

5.1.1.4. A copy of the record;

5.1.1.5. Any internal records or coordination actions relating to the denial; (6) the denial authority's comments on the appellant's arguments; and (7) the legal reviews.

5.1.2. If the denial authority reverses an earlier denial and grants access or amendment, notify the requester immediately.

5.1.3. The system manager may include a brief summary of the reasons for not amending the record. Limit the summary to the reasons SAF/GCA gave to the individual. The summary is part of the individual's record, but it is not subject to amendment procedures.

5.1.4. AFLOA/JACL reviews the denial and provides a final recommendation to SAF/GCA. SAF/GCA provides the requester the final Air Force decision and explains judicial review rights.

5.1.5. SAF/GCA will provide a copy of the decision letter to the HAF/MAJCOM/FOA/DRU Privacy Act Officer if applicable and the originating Privacy Act Officer to close the case file.

5.1.6. The records will clearly show that a statement of disagreement is filed with the record or separately, if applicable.

5.1.7. The disputed part of the record must show that the requester filed a statement of disagreement.

5.1.8. Give copies of the statement of disagreement to the record's previous recipients. Inform subsequent record users about the dispute and give them a copy of the statement with the record.

Chapter 6

DISCLOSING RECORDS TO THIRD PARTIES

6.1. Disclosure Considerations.

6.1.1. Placing Personally Identifiable Information on Shared Drives. PII contained in any records shall not be placed on shared drives for access by groups of individuals unless each person of the group has an official need to know for an approved government purpose to perform their job. Add appropriate access controls to ensure access by only authorized individuals that have the need to know.

6.1.1.1. Recall rosters will be marked FOUO and only provided to individuals with a need to know of the information in order to accomplish their official duties. Do not place a complete recall roster on a shared location with access allowed for everyone in a unit, unless necessary for official purposes.

6.1.2. Placing PII Files in Collaborative IT Environments. AF ISOs of collaborative IT environments within the USAF enterprise, i.e., Microsoft SharePoint, Tracking Management Tool (TMT), Customer Relations Management (CRM), share drives, etc., will adhere to this Instruction and Records Management business rules established for particular categories of official records.

6.1.2.1. The ISO will obtain written permission from the ISO of the parent system of records before placing electronic files or records copies into a collaborative or shared environment.

6.1.2.2. The ISO will protect, safeguard and manage Privacy Act records and records containing PII within a shared environment according to the published SORN and/or PIA of the parent system of records from which electronic files and records copies are shared. AF SORNs are posted on the Defense Privacy Office public website **http://privacy.defense.gov/notices/usaf**. AF PIAs are posted on the Air Force Privacy Act public website **http://www.privacy.af.mil/pia/index.asp**.

6.1.3. Personal Information That Requires Protection. Following are some examples of information that is normally not releasable to the public without the written consent of the subject. This list is not all-inclusive. The facts and circumstances of the request and the nature of the record will determine releasability.

6.1.3.1. Marital status (single, divorced, widowed, separated).

6.1.3.2. Number, name, and sex of dependents.

6.1.3.3. Civilian educational degrees and major areas of study (unless the request for the information relates to the professional qualifications for Federal employment).

6.1.3.4. School and year of graduation (if in connection with professional qualifications for Federal employment).

6.1.3.5. Home of record.

6.1.3.6. Home address and phone.

6.1.3.7. Age and date of birth (year).

6.1.3.8. Present or future assignments for overseas or for routinely deployable or sensitive units.

6.1.3.9. Office, name, state, unit address and duty phone for overseas or for routinely deployable or sensitive units.

6.1.3.10. Race/ethnic origin.

6.1.3.11. Educational level (unless the request for release of the information relates to the professional qualifications for Federal employment).

6.1.3.12. Social Security Number.

6.2. Releasable Information. Following are examples of information normally releasable to the public without the written consent of the subject. This list is not all-inclusive. Since 2001 the release of names and other PII of certain DoD personnel are given more scrutiny and the interests supporting withholding of the information given more weight. See **http://www.DoD.mil/pubs/foi/dfoipo/docs/names_removal.pdf**.

6.2.1. Name of personnel above the O-6 grade or the civilian equivalent.

6.2.2. Rank.

6.2.3. Grade.

6.2.4. Air Force specialty code.

6.2.5. Pay (including base pay, special pay, all allowances except Basic Allowance for Quarters and Variable Housing Allowance).

6.2.6. Gross salary for civilians.

6.2.7. Past duty assignments, unless sensitive or classified.

6.2.8. Present and future approved and announced stateside assignments.

6.2.9. Position title.

6.2.10. Office, unit address, official e-mail address, and duty phone number (CONUS only).

6.2.11. Date of rank.

6.2.12. Entered on active duty date.

6.2.13. Pay date.

6.2.14. Source of commission.

6.2.15. Professional military education.

6.2.16. Promotion sequence number.

6.2.17. Military awards and decorations.

6.2.18. Duty status of active, retired, or reserve.

6.2.19. Active duty official attendance at technical, scientific, or professional meetings.

6.2.20. Biographies and photos of senior personnel above the rank of O-6 or civilian equivalent.

6.2.21. Date of retirement, separation.

6.3. Disclosing Information. In all cases, use the following guidelines to decide whether to release information:

6.3.1. Would the subject have a reasonable expectation of privacy in the information requested?

6.3.2. Is disclosing the information in the public interest? The public interest relates to how the Air Force carries out its statutory and regulatory duties.

6.3.3. Balance the public interest against the individual's privacy interest. Do *not* consider the requester's purpose, circumstances, or proposed use.

6.4. Rules for Releasing Privacy Act Information Without Consent of the Subject. The Privacy Act prohibits disclosing disclosure of any Privacy Act records without the written consent of the individual to whom the record pertains. There are twelve exceptions to the "no disclosure without consent" rule. **http://www.privacy.af.mil/exceptions/index.asp**.

6.5. Disclosing the Medical Records of Minors. Air Force personnel may disclose the medical records of minors to their parents or legal guardians in conjunction with applicable Federal laws and guidelines. The laws of each state define the age of majority. Consult with the servicing legal office and Military Treatment Facility (MTF) for guidance in regard to the age of majority in overseas locations.

6.6. Disclosure Accountings. System managers must keep an accurate record of all disclosures made from any system of records except disclosures to DoD personnel for official use or disclosures under the FOIA. System managers may use AF Form 771, Accounting of Disclosures. Retain disclosure accountings for 5 years after the disclosure, or for the life of the record, whichever is longer.

6.6.1. System managers shall file the Accounting of Disclosure record and give it to the subject on request, send corrected or disputed information to previous record recipients, explain any disclosures, and provide an audit trail for reviews. Include in each accounting:

6.6.1.1. Release date.

6.6.1.2. Description of information.

6.6.1.3. Reason for release.

6.6.1.4. Name and address of recipient.

6.6.2. Some exempt systems let you withhold the accounting record from the subject.

6.6.3. You may withhold information about disclosure accountings for law enforcement purposes at the law enforcement agency's request.

6.7. Computer Matching. Computer matching programs electronically compare records from two or more automated systems that may include DoD, another Federal agency, state or other local government. A system manager proposing a match that could result in an adverse action against a Federal employee must meet these requirements of the Privacy Act: (1) prepare a written agreement between participants; (2) secure approval of the Defense Data Integrity Board; (3) publish a matching notice in the *Federal Register* before matching begins; (4) ensure full investigation and due process; and (5) act on the information, as necessary.

6.7.1. The Privacy Act applies to matching programs that use records from: Federal personnel or payroll systems and Federal benefit programs where matching: (1) determines Federal benefit eligibility; (2) checks on compliance with benefit program requirements; (3) recovers improper payments or delinquent debts from current or former beneficiaries.

6.7.2. Matches used for statistics, pilot programs, law enforcement, tax administration, routine administration, background checks and foreign counterintelligence, and internal matching that won't cause any adverse action are exempt from Privacy Act matching requirements.

6.7.3. Any activity that expects to participate in a matching program must contact SAF/A6PPF immediately. System managers must prepare a notice for publication in the *Federal Register* with a Routine Use that allows disclosing the proposed system notice to SAF/A6PPF. Allow 180 days for processing requests for a new matching program.

6.7.4. The subjects of a Privacy Act record must receive a PAS when personal information the subjects are asked to provide will be used in a matching program as a routine use. The most appropriate method of doing so is to include the PAS on the form used to apply for benefits. Coordinate appropriate statements with the appropriate HAF/MAJCOM/FOA/DRU Privacy Officer and SAF/A6P.

6.8. Privacy and the Web. Do not post PII on publicly accessible DoD web sites unless authorized by law and implementing regulation and policy. Additionally, do not post PII on .mil private web sites unless authorized by the local commander, for official purposes, and an appropriate risk assessment is performed. See AFI 33-129 *Transmission of Information Via the Internet*.

6.8.1. Add a prominent Privacy Act Advisory at web site entry points. A Privacy Act Advisory is required to be posted on the web page where the information is being solicited or through a well-marked hyperlink whenever a web site solicits PII, even when not retained by the site after login or maintained in a Privacy Act system of records. Notices must clearly explain when the collection of PII is voluntary and notify users how to provide consent.

6.8.2. Include a Privacy Act Statement on the web page if it collects information directly from an individual that is maintained and retrieved by his or her name or personal identifier (i.e., SSN). Only maintain such information in approved Privacy Act systems of records that are published in the *Federal Register*. The Privacy Act gives subject individual's certain rights with respect to the government's maintenance and use of PII collected about them that is contained in a Privacy Act record. Provide a link to the Air Force Privacy Act policy and SORNs at **http://www.privacy.af.mil**/ and **http://www.defenselink.mil/privacy/notices/usaf**.

Chapter 7

PRIVACY IMPACT ASSESSMENTS

7.1. Evaluating Information Systems for Privacy Act Compliance and Risk Identification. ISOs, PMs, and IAMs will address Privacy Act requirements and risks to Privacy Act data and plan the integration of privacy protections with appropriate IA controls into the development life cycle of an information system. A PIA will be completed in accordance with DoDI 5400.16, *DoD Privacy Impact Assessment (PIA) Guidance*, February 12, 2009.

7.2. What is a PIA? The Privacy Impact Assessment is an analysis of how PII information is handled: (1) to ensure PII handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (2) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (3) to examine and evaluate protections and alternative processes for handling PII information to mitigate potential privacy risks.

7.2.1. The PIA identifies the physical, technical, and administrative controls that are needed to protect PII. Information Assurance (IA) controls are identified in DoDI 8500.2, *Information Assurance (IA) Implementation*, 6 Feb 03 that mitigate specific risks that will be implemented and tested before deployment or release of the system; and whether a SORN exists, needs to be created, and/or needs to be amended. The *E-Government Act of 2002* and DoDI 5400.16 requires PIAs to be conducted ***before***:

7.2.1.1. Developing or procuring IT systems or projects that collect, maintain, or disseminate information in identifiable form from or about individuals as defined in DoD 5400.11-R

7.2.1.2. PIAs are required to be performed, accomplished and/or updated as necessary when a system change exposes a new privacy risk for which an IA control must be identified and tested before re-deployment or re-release of the system.

7.2.1.3. The depth and content of the PIA should be thorough and appropriate for the nature of the information to be collected and the size and complexity of the information technology system.

7.3. When a PIA is required. PIAs are submitted 120 days from the scheduled operational and expiration date on all new and existing systems meeting the criteria when PII is collected, maintained, used, or disseminated in electronic form about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally, in order to:

7.3.1. Ensure PII handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;

7.3.2. Determine the need, privacy risks, and effects of collecting, maintaining, using, and disseminating PII in electronic form; and

7.3.3. Examine and evaluate protections and alternative processes to mitigate potential privacy risks.

7.4. When a PIA is not required. A PIA is not required when: (1) PII is not being maintained, collected, store, used, and/or disseminated other than the user table or (2) the system is an approved National Security System (NSS). Administrative and personnel systems that do not meet one or more of the NSS conditions are not exempt from the PIA requirement.

7.5. Who conducts the PIA? The ISO will conduct a PIA in conjunction with the system PM, system IAM and local/functional Privacy Official.

7.5.1. Medical IT systems that are Defense Health Program (DHP) funded or in the AF line-funded portfolio and managed by AFMS assets, shall route PIAs through the AF SG-CIO office for appropriate management, signatures, and oversight.

7.5.2. All DoD Medical Department IT systems purchased with DHP funds must ONLY be reported to the DoD Information Technology Portfolio Repository (DITPR) via the component Tricare Management Activity (TMA).

7.6. Format and Digital Signatures. All PIAs shall be completed on DD Form 2930 as an *unsecured* fillable PDF which requires digital signatures as follows, except for medical DHP funded systems (see paragraph **7.5.1**):

7.6.1. Obtain the first three signatures before email submission to SAF/A6PPF **AirForcePrivacy@pentagon.af.mil** for review by SAF/A6 and digital signatures in the final three blocks.

7.6.2. The system Program Manager.

7.6.3. The system Information Assurance Manager.

7.6.4. The HAF/MAJCOM/FOA/DRU Privacy Official.

7.6.5. The Senior Information Assurance Official (SIAO) or designee.

7.6.6. The Senior Agency (AF) Privacy Official (SAOP) or designee.

7.6.7. The AF CIO as final reviewer.

7.7. Submitting Approved PIAs. Approved PIAs on IT systems that collect PII on members of the General Public will be further submitted to the Office of the Secretary of Defense, Chief Information Officer (OSD NII/CIO) as they are required for submission to OMB; otherwise submission is required only to AF. All approved and signed PIAs will be redacted in Sections 3 and 4 of information which shall not be posted, i.e., vulnerabilities and risk mitigations, classified, sensitive, and non-releasable or PII contained in an assessment. It is then posted on the AF Privacy Act public access website **http://www.privacy.af.mil/pia/index.asp** and email notification sent to the originator.

Chapter 8

PREPARING SYSTEM OF RECORDS NOTICE (SORN) FOR PUBLISHING IN THE FEDERAL REGISTER

8.1. Publishing System of Records Notices (SORNs). Records that are retrieved by name or personal identifier are subject to Privacy Act requirements and are referred to as Privacy Act Systems of Records. The Air Force must publish SORNs in the *Federal Register*, describing the collection (noun) of information for new, changed or deleted systems to inform the public and allow a 30 day opportunity for public comment. During this 30 day review period, the system owner shall not collect, store, use, or disseminate the information to be used. System owners can begin collecting, storing, using, and disseminating PII on the *Federal Register* published effective date unless comments are received that would result in a contrary determination.

8.2. When is a SORN required? A SORN is required for system of records that are retrieved by name or personal identifier. The Privacy Act requires submission of new or significantly changed SORNs to the Office of Management and Budget (OMB) and both houses of Congress before publication in the *Federal Register*. This applies when:

8.2.1. Starting a new system. (Add)

8.2.2. Instituting significant changes to an existing system. (Alter or Amend)

8.2.3. Sending out data collection forms or Instructions.

8.2.4. Issuing a request for proposal or invitation for bid to support a new system.

8.2.5. Other Systems**.** National Security Privacy Act Systems of Records require that a SORN be completed, as with any other SORN. While some or many of these systems may be classified, the SORN is written in an unclassified manner describing the nature of the collection of PII. (See DoD 5400.11-R, for the use and establishment of exemptions that may apply to these systems).

8.3. Adopting Existing SORNs. A new system of records may "piggy back" onto an existing published SORN:

8.3.1. First, research current SORNs, including those that cover systems of records government-wide and DoD-wide on the Defense Privacy Notices website **http://privacy.defense.gov/notices/osd** and the Air Force Privacy Notices website **http://privacy.defense.gov/notices/usaf** for one that matches well with the new system of records at all points, i.e., Category of Individuals Covered, Category of Records, Authority, Purposes, Routine Uses, Policies, etc.

8.3.2. Second, if necessary, contact the current SORN owner through the POC information on the SORN to discuss altering or amending their SORN to include the new system of records and POC information.

8.3.3. Provide the system owner the altered or amended SORN for their review and processing.

8.4. Updating SORNs. Examples for Adding, Altering, Amending, and Deleting a SORN are available on the FOIA/Privacy Act Community of Practice (COP)

https://afkm.wpafb.af.mil/community/views/home.aspx?Filter=OO-SC-AF-53 listed under *Privacy Act Procedures, System of Records Notifications*. Use Microsoft Word and the Track Changes tool in MS Word to indicate additions and changes to existing notices.

8.5. Submitting SORNs for Publication in the *Federal Register.* The PM must submit the proposed SORN through the local and HAF/MAJCOM/FOA/DRU Privacy Office a minimum of 120 days before the planned implementation date of a new system of records or a change to an existing system of records subject to this Instruction. The HAF/MAJCOM/FOA/DRU Privacy Office will review for accuracy and completeness and send electronically to the AF Privacy Office **AirForcePrivacy@pentagon.af.mil** . The AF Privacy Office will review and forward to the Defense Privacy Office for publishing in the *Federal Register*, as appropriate.

8.6. Requirement for Periodic Review of Published SORNs. System PMs will annually review to validate currency of their published SORNs coinciding with annual FISMA reviews and submit any changes through the process described in this chapter and promptly update appropriate answers to EITDR questions.

8.7. Deletion of SORNs. If your records system is decommissioned or closed and has a published SORN, comply with DoD 5400.11-R, "Deletion of System of Records Notices" and submit appropriate amendment or deletion through the AF Privacy Office **AirForcePrivacy@pentagon.af.mil** to be forwarded to Defense Privacy Office for publishing in the *Federal Register*.

Chapter 9

PROTECTING AND DISPOSING OF RECORDS

9.1. Protecting Records. Protecting privacy information is the responsibility of every federal employee, military member, and contractor who handles privacy records or PII contained in any record.

9.2. Guidance on Protecting PII. It is AF policy that all PII shall be evaluated by the ISO for impact of loss or unauthorized disclosure and protected accordingly. Ensure coordination is accomplished between IT system PMs, IAMs and Privacy Officials. (AFI 33-200) (DoDI 5400.16).

9.2.1. Assigning PII High or Moderate Impact Security Category (SC). All electronic systems of records shall be assigned a High or Moderate PII impact security category according to the definitions established in this Instruction and Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, Feb 2004. **http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf**.

9.2.2. Protect PII of High or Moderate impact security category at a Confidentiality Level of Sensitive or higher as established in DoDI 8500.2, **http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf** unless specifically cleared for public release (e.g., the name and contact information for selected senior officials or personnel whose duties require regular contact with the public).

9.2.2.1. As early as possible in the life cycle of IT-dependent programs, information owners shall establish the mission assurance category, security classification, sensitivity, and need-to-know of information and information systems.

9.2.2.2. Information system owners shall establish the permissible uses of information and associated mission or business rules of use, and ensure that the distinction is clear to all personnel between information that is operationally sensitive and information that can be made available to the public.

9.2.2.3. Mission assurance category establish the requirements for availability and integrity, and security classification, sensitivity, and need-to-know establish confidentiality requirements.

9.2.2.4. Enclosure 4 of DoDI 8500.2 provides detailed lists of the IA Controls necessary to achieve the baseline levels of availability, integrity, and confidentiality for mission assurance category and classification. Any Mission Assurance Category is acceptable for DoD and AF information systems processing PII.

9.2.2.5. Electronic PII records that are assigned a High Impact Category shall be protected as follows:

9.2.2.5.1. Such records *shall not be routinely* processed or stored on mobile computing devices or removable electronic media without written approval of the Information Security Officer (ISO).

9.2.2.5.2. Except for compelling operational needs, any mobile computing device or removable electronic media that processes or stores High Impact PII electronic records (e.g., containing SSN) *shall be restricted to workplaces* that minimally satisfy Physical and Environmental Controls for Confidentiality Level Sensitive as established in DoDI 8500.2 (hereinafter referred to as "protected workplaces").

9.2.3. Mobile Computing Devices. Any mobile computing or storage device containing High Impact PII electronic records removed from protected workplaces, including those approved for routine processing, shall:

9.2.3.1. Be signed in and out with a supervising official designated in writing by the organization security official.

9.2.3.2. Use an AFVA 33-276, *Privacy Act Label*, to assist in identifying and protecting Privacy Act information by placing the label on the covers of removable electronic storage media. Do not place the label directly on equipment.

9.2.3.3. Require certificate based authentication using a DoD or DoD-approved PKI certificate on an approved hardware token to access the device.

9.2.3.4. Implement IA Control PESL-1 (Screen Lock), with a specified period of inactivity not to exceed 30 minutes (15 minutes or less recommended).

9.2.3.5. PII Data at Rest on Mobile Devices. Encrypt all data at rest, i.e., data that is contained on hard drives or other storage media within mobile devices as well as all removable media created by or written from the device while outside a protected workplace. If a mobile device is incapable of encryption, it cannot be used to store PII. Minimally, the cryptography shall be NIST-certified (i.e., FIPS 140-2 **http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf**). See DoDI 8500.2, ECCR (Encryption for Confidentiality (Data at Rest)).

9.2.4. PII and Remote Access. Only DoD authorized devices shall be used for remote access. Any remote access, whether for user or privileged system administrator functions, must conform to both IA Control EBRU- 1 (Remote Access for User Functions) and EBRP- 1 (Remote Access for Privileged Functions) as established in DoDI 8500.2. and DoD Memorandum, *Department of Defense Guidance on Protecting Personally Identifiable Information (PII)*, 18 Aug 2006:

9.2.4.1. Remote access to High Impact PII electronic records is discouraged, is permitted only for compelling operational needs, and:

9.2.4.2. Shall employ certificate based authentication using a DoD or DoD-approved PIU certificate on an approved hardware token.

9.2.4.3. The remote device gaining access shall conform to IA Control PESL- 1 (Screen Lock), with a specified period of inactivity not to exceed 30 minutes (1 5 minutes or less recommended). See DoDI 8500.2.

9.2.4.4. The remote device gaining access shall conform to IA Control ECRC-1, Resource Control. See DoDI 8500.2.

9.2.4.5. Download and local/remote storage of PII records is prohibited unless expressly approved by the ISO.

9.3. PII Breach Reporting. Refer to OSD Memorandum, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, 05 Jun 09, Appendix A, Table 1, PII Incident Reporting and Risk Assessment Model. A PII breach is defined as "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." (see Attachment 1, Terms). Breaches must be reported to the installation Privacy Official by anyone discovering it.

9.3.1. The installation Privacy Official will submit a Preliminary PII Incident Report by unencrypted email according to the timeline below:

9.3.1.1. PII Incident Reports must be completed in the format provided by the Defense Privacy Office located on the Air Force Privacy COP: **https://afkm.wpafb.af.mil/ASPs/docman/DOCMain.asp?Tab=0&FolderID=OO-SC-AF-53-5-4&Filter=OO-SC-AF-53**

9.3.1.2. Use for Preliminary and Final reports.

9.3.1.3. Use Red color font for changes made.

9.3.1.4. Reports must include names of individuals involved or affected by the breach. Reports are forwarded by unencrypted email through the appropriate HAF/MAJCOM/FOA/DRU Privacy Office to **AirForcePrivacy@pentagon.af.mil.**

9.3.1.5. Within one hour of the discovery of the PII breach the installation Privacy Official will ensure the United States Computer Emergency Readiness Team (US CERT) has been notified in accordance with the requirements and guidance at **www.us-cert.gov**.

9.3.1.6. Within 24 hours of the PII breach the installation Privacy Official will notify the senior-level individual in the chain of command of the unit where the incident occurred and simultaneously notify the HAF/MAJCOM/FOA/DRU Privacy Officer by official unencrypted email attaching the written PII Incident Preliminary Report.

9.3.1.7. Within 24 hours of being notified of the PII breach the HAF/MAJCOM/FOA/DRU Privacy Official (as appropriate) will notify the Air Force Privacy Office by official unencrypted email attaching the written PII Incident Preliminary Report.

9.3.1.8. Within 48 hours of the PII breach notification the AF Privacy Act Officer will forward the report to the DoD Privacy Official and concurrently notify the Senior Agency Official for Privacy (SAOP).

9.3.1.9. Resolving the PII Incident. The underlying breach that led to the breach shall continue to be reported to the AF Privacy Office in accordance with these reporting procedures until resolved. However, corrective actions will be taken immediately to provide required protection of PII.

9.3.1.10. The installation Privacy Official will send the PII Incident Final Report when resolved in the same routing as previous notifications.

9.3.2. Guidelines for conducting an inquiry of a PII Incident. The senior-level individual who is in the chain of command for the organization where the loss, theft or compromise occurred will appoint another official to conduct an inquiry on the PII incident to determine the cause of the breach and if a criminal investigation is warranted.

9.3.2.1. The installation Privacy Official will provide the guidance to the individual appointed to properly complete the PII Incident Final Report and reference AF and DoD Policies and the Privacy Act for use in completing the investigation as required.

9.3.2.2. The appointed official will review the initial PII Incident Preliminary Report and independently assess the handling of the breach. They will make clarifications and additions on the PII Incident Final Report as required, and submit to the appointing senior-level individual a recommendation of whether notification to affected individuals is required after a risk assessment analysis has been completed along with any corrective actions that should be taken. A legal review may be requested before submission of the Final Report to determine whether administrative, disciplinary action or a criminal investigation is warranted and appropriate. The appointed official may be asked by the appointing senior-level individual to make additional recommendations or more formal reports as required.

9.3.2.3. Upon concurrence with PII Incident Final Report recommendations, the senior-level individual who is in the chain of command for the organization where the loss, theft or compromise occurred will route the Final report to the appropriate Privacy Office.

9.3.3. Air Force Computer Emergency Response Team (AFCERT) Reported PII Incidents. According to CJCSM 6510.01A, Enclosure C, Paragraph 7.b, "when a Computer Network Defense Service Provider (CNDSP) discovers compromised or potentially compromised PII, they must notify the US CERT and their Service Privacy Office POC."

9.3.3.1. AFCERT will follow through on CNDSP detections of PII Incidents by notifying the ISO and PM of the web application and/or IT system cited.

9.3.3.2. ISO and PM of web application and/or IT system responsible for the PII breach must notify the installation Privacy Official or HAF/MAJCOM/FOA/DRU Privacy Official who will accomplish PII Breach notifications as established by this AF policy and DoD reporting guidance. (See paragraph 9.3) AF Privacy Officials are located throughout the Air Force to respond routinely to PII Incidents and provide assistance to commanders and organizations with PII Incident reporting and notifications.

9.3.3.3. Notification to affected individuals, if determined to be required, will be made no later than 10 working days after a PII breach is discovered and the identities of the affected individuals ascertained by a senior level individual in the chain of command for the organization where the breach occurred. A senior-level official is considered to be at a Directorate or higher level. Military Group or higher level commanders of the O-6 rank or above also meet the definition of "senior level." (See Attachment 7, Privacy Breach Notification Letter).

9.4. Risk Based Management. Apply a risk based management approach. Evaluate the effectiveness of additional protections against sensitivity, probability of exposure, risk and cost.

9.4.1. Consider the sensitivity category (Low, Moderate or High) of the PII and the probability of exposure, risk of disclosure, loss or alteration when providing physical security measures. (See Attachment **5**, Risk Notification.)

9.4.2. Information marked For Official Use Only (FOUO) or Controlled Unclassified Information (CUI) must be protected from unauthorized disclosure. Reasonable steps shall be taken both during and after working hours to minimize risk of access by unauthorized personnel. DoD 5200.1-R, Appendix 3 addresses the protection of CUI and AFI 31-401 addresses FOUO.

9.4.3. AF Form 3227 or DD Form 2923, Privacy Act Cover Sheet. Use is mandatory with Privacy Act materials when removed from their system of record or when not within their protected workplace. Use it to cover and protect PII contained in other records at all times from casual viewing in office environments and other areas that are accessible to many individuals who may not have a need to know the PII in the performance of their duties.

9.4.4. AFVA 33-276. Privacy Act Label. Use is mandatory to assist in identifying and protecting Privacy Act information by placing the label on the covers of removable electronic storage media such as Laptops, Government Hard drives, DVDs, CDs, diskettes, and tapes. The label is not authorized for use on file drawers or file folders, cabinets, mobile electronic devices, or other stationary equipment or materials.

9.5. Disposing of Records. Consult a Records Professional before disposing of any records. You may use the following methods to dispose of records protected by the Privacy Act for authorized destruction according to RDS maintained in the Air Force Records Information Management System (AFRIMS).

9.5.1. Destroy by any reasonable method that prevents loss, theft or compromise during and after destruction such as pulping, macerating, tearing, burning, shredding or otherwise completely destroying the media so that PII is both not readable and is beyond reconstruction. The shreds or particles cannot be read. The shreds or particles cannot be reconstructed. Refer to NIST SP800-88. **http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf**

9.5.2. Degauss or overwrite magnetic media according to established guidelines. DoD 5200-1 and AFI 31-401 also govern destruction of FOUO and CUI.

9.5.3. Recycling of material protected under the Privacy Act.

9.5.3.1. When safeguarding information protected under the Privacy Act can be assured as described in this chapter, disposal of recyclable Privacy Act protected products may be accomplished through the Defense Reutilization and Marketing Office (DRMO) or through contracted recycling providers that manage a base-wide recycling program.

9.5.3.2. Originators of material protected under the Privacy Act must safeguard it until it is transferred to the recycling provider. This transfer does not require a disclosure accounting.

Chapter 10

PRIVACY ACT EXEMPTIONS

10.1. Exemption Types. This chapter contains the most current exemptions that have been published as final rules for the listed systems of records as of the date of this AFI. The ISO should ensure that a more recent final rule has not been published. There are two types of exemptions from release or disclosure permitted by Title 5 USC 552a:

10.1.1. *A General exemption* authorizes the exemption of a system of records from most parts of the Privacy Act.

10.1.2. *A Specific exemption* authorizes the exemption of a system of records from only a few parts of the Privacy Act.

10.2. Authorizing Exemptions. Denial authorities may withhold release or disclosure of records to the first party requesters using Privacy Act exemptions *only* when an exemption for the system of records has been published in the *Federal Registe*r as a final rule. See **http://privacy.defense.gov/notices/usaf**; exemptions are noted in the right column.

10.3. Requesting an Exemption. An ISO who believes that a system requires an exemption from some or all of the requirements of the Privacy Act will send a request through the Wing Privacy Office, the HAF/MAJCOM/FOA/DRU or FOA Privacy Office, to AF Privacy Office, SAF/A6PPF. Final approval is by the DoD Privacy Officer. The request will detail the reasons why the exemption applies, the section of the Act that allows the exemption, and the specific subsections of the Privacy Act from which the system is to be exempted, with justification for each subsection.

10.4. Exemptions. Exemptions permissible under title 5 are located at **http://uscode.house.gov/search/criteria.shtml**:

10.4.1. The (j) (2) exemption. Applies to investigative records created and maintained by law-enforcement activities whose principal function is criminal law enforcement.

10.4.2. The (k) (1) exemption. Applies to information specifically authorized to be classified according to DoD 5200.1R, *Information Security Program*.

10.4.3. The (k) (2) exemption. Applies to investigatory information compiled for law-enforcement purposes by non-law enforcement activities and which is not within the scope of the (j) (2) exemption. However, the Air Force must allow an individual access to any record that is used to deny rights, privileges or benefits to which he or she would otherwise be entitled by Federal law or for which he or she would otherwise be eligible as a result of the maintenance of the information (unless doing so would reveal a confidential source).

10.4.4. The (k) (3) exemption. Applies to records maintained in connection with providing protective services to the President and other individuals under Title 18; Crimes and Criminal Procedure, USC, section 3056; Powers, authorities, and duties of United States Secret Service.

10.4.5. The (k) (4) exemption. Applies to records maintained solely for statistical research or program evaluation purposes and which are not used to make decisions on the rights, benefits, or entitlement of an individual except for census records which may be disclosed

under Title 13, CENSUS, U.S.C., Section 8; Authenticated transcripts or copies of certain returns; other data; restriction on use; disposition of fees received.

10.4.6. The (k) (5) exemption. Applies to investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information, but only to the extent such material would reveal the identity of a confidential source. This provision allows protection of confidential sources used in background investigations, employment inquiries, and similar inquiries that are for personnel screening to determine suitability, eligibility, or qualifications.

10.4.7. The (k) (6) exemption. Applies to testing or examination material used solely to determine individual qualifications for appointment or promotion in the federal or military service, if the disclosure would compromise the objectivity or fairness of the test or examination process.

10.4.8. The (k) (7) exemption. Applies to evaluation material used to determine potential for promotion in the Military Services, but only to the extent that the disclosure of such material would reveal the identity of a confidential source.

Chapter 11

TRAINING

11.1. Who Needs Training. The Privacy Act requires that all DoD and pertinent contractor personnel involved in the design, development, operation and maintenance of any system of records be trained annually in the principles and requirements of the Privacy Act; personnel who may be expected to deal with the news media or the public, as well as personnel specialists, finance officers, information managers, supervisors, and individuals working with medical, personnel, finance and security records. Privacy Act annual refresher training is also required. Training shall include rules of behavior and consequences when rules are not followed. Emphasis shall be made of the penalties and fines related to violations of the Privacy Act. Additional or advanced training should be provided commensurate with increased responsibilities or change in duties.

11.1.1. Commanders/Directors shall ensure that training and communication related to privacy and security is job specific and commensurate with an individual's responsibilities. Such training shall be a prerequisite before an employee, military member, or contractor is permitted to access DoD information systems that contain Privacy Act material. Such training is mandatory for AF military personnel, employees and managers, and shall include contractors and business partners. Training must be provided and documented by the Privacy Officer/Monitor.

11.1.2. Commanders shall ensure their personnel receive the following Privacy training:

11.1.2.1. Orientation Training. Training that provides individuals with a basic understanding of the requirements of the Privacy Act as it applies to the individual's job responsibilities. The training shall be provided to all personnel and as a prerequisite to all other levels of Privacy training.

11.1.2.2. Specialized Training**.** Training that provides information as to the application of specific provisions of this Instruction to specialized areas of job performance. Personnel of particular concern include, but are not limited to personnel specialists, finance officers, special investigators, paperwork managers, public affairs officials, IT professionals, and any other personnel responsible for implementing or carrying out functions under this Instruction.

11.1.2.3. Management Training. Training that provides managers and decision makers considerations that they should take into account when making management decisions regarding actions under the Privacy Program.

11.1.2.4. Privacy Act Systems of Records Training. Ensure all individuals who work with a Privacy Act system of records are trained on the provisions of the Privacy Act systems of records notice and this Instruction. Stress individual responsibilities and advise individuals of their rights and responsibilities under this Instruction and penalties under the Privacy Act.

11.1.2.5. Annual Refresher Training. Provide annual refresher training to ensure employees and managers, as well as contractor personnel, continue to understand their Privacy Act responsibilities. All federal personnel with authorized access to PII shall

annually complete refresher training prior to granting access. An annual training certificate shall be provided at the completion of annual refresher training online. Retain certificates in either the AF centralized electronic training record, personnel record, or in the training manager office to which the employee is assigned. When contractor personnel are involved, retain certificates in the training office of the appropriate AF activity supported by the contract.

11.2. Privacy Act Training Tools. Helpful resources include:

11.2.1. The Air Force FOIA and Privacy Act web page includes a Privacy Overview, Privacy Act training slides, the Air Force SORNs, and links to the Defense Privacy Board Advisory Opinions, the DoD and Department of Justice Privacy web pages. Go to **http://www.foia.af.mil** . Click on "Resources" and/or "Privacy Act", **http://www.privacy.af.mil/index.asp** and "Training." **http://www.privacy.af.mil/training/index.asp** .

11.2.2. "*The Privacy Act of 1974*," a 32-minute film developed by the Defense Privacy Office. Contact the Joint Visual Information Services Distribution Activity at DSN 795-6543 or commercial (570) 895-6543, and ask for #504432 "*The Privacy Act of 1974*."

11.2.3. A Manager's Overview, *What You Need to Know About the Privacy Act*. This overview gives you Privacy Act 101 and is available on-line at **http://www.privacy.af.mil/training/index.asp** .

11.2.4. Training slides for use by the HAF/MAJCOM/FOA/DRU and base PRIVACY ACT officers, available from the FOIA web page at **http://www.foia.af.mil** , under "Resources."

11.2.5. DISA web based training service ADLS. An authorized user on the .mil domain can go directly to ADLS **https://golearn.csd.disa.mil** "Course List" for "Total Force Awareness Training" then "Information Protection" which includes mandatory Privacy Act and Information Assurance annual refresher course and a PII course at **http://iase.disa.mil/eta/index.html#onlinetraining**.

11.3. Information Collections, Records, and Forms or electronic versions.

11.3.1. Information Collections. No information collections are required by this publication.

11.3.2. Records. Retain and dispose of Privacy Act records according to disposition Instructions in the SORN (SORN), which will be consistent with the RDS maintained in AFRIMS. **https://www.my.af.mil/afrims/afrims/afrims/rims.cfm**

11.4. Adopted Forms. DD Form 67, *Form Processing Action Request***,** DD Form 2923, *Privacy Act Data Cover Sheet***,** DD Form 2930**,** *Privacy Impact Assessment***,** AF Form 624, *Base/Unit Locator and PSC Directory*, and AF Form 847, *Recommendation for Change of Publication*.

11.5. Prescribed Forms. AF Form 771, *Accounting of Disclosures*, AF Form 3227, *Privacy Act Cover Sheet.*

WILLIAM T. LORD, Lt Gen, USAF

Chief of Warfighting Integration and Chief Information Officer

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Title 5 USC Section 552a, as amended, *The Privacy Act of 1974*

Title 5 USC Section 552, as amended, *The Freedom of Information Act of 1966, as Amended*

Title 10 USC Section 8013, *Secretary of the Air Force*

Title 10 USC Section 130b, *Personnel in Overseas, Sensitive, or Routinely Deployable Units*

Executive Order 9397, *Numbering System for Federal Accounts Relating to Individual Persons*, November 30, 1943

Executive Order 13478, *Amendments To Executive Order 9397 Relating To Federal*

Agency Use of Social Security Numbers, November 18, 2008

Public Law 100-235, *The Computer Security Act of 1987*

Public Law 107-347, Section 208, *E-Government Act of 2002, Federal Information Security Management Act (FISMA)*

DoD 5200.1-R, *Information Security Program*, January 14, 1997

DoD 5400.7-R/AFMAN 33-302, *DoD Freedom of Information Act Program*, October 21, 2010

DoD 5400.11- R, *DoD Privacy Program*, May 14, 2007

DoD 6025.18R, *DoD Health Information Privacy Regulation*, January 24, 2003

DoD 5100.3, *Support of the Headquarters of Combatant and Subordinate*

Joint Commands, March 24, 2004

DoDI 5400.16, *DoD Privacy Impact Assessment (PIA) Guidance*, February 23, 2009

DoDI 8500.2, *Information Assurance (IA) Implementation*, February 6, 2003

AFI 33-129, *Transmission of Information Via the Internet*, February 3, 2005

AFI 33-200, *Information Assurance Management*, December 23, 2008

AFI 33-360, *Publications and Forms Management*, May 18, 2006

AFMAN 33-363, *Management of Records*, March 1, 2008

Air Force Records Information Management System (AFRIMS)

Air Force Visual 33-276, *Privacy Act Label*, August 1, 2000

Directive-Type Memorandum (DTM) 07-015-USD (P&R), *DoD Social Security Number (SSN) Reduction Plan*, 28 Mar 2008;

Federal Information Processing Standard (FIPS) 140-2, *Security Requirements For Cryptographic Modules*, 25 May 2001;

Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004;

Abbreviations and Acronyms

AFCERT—Air Force Computer Emergency Response Team

AF CIO—Air Force Chief Information Officer

AFBCMR—Air Force Board for Correction of Military Records

AFLOA—Air Force Legal Operations Agency

AFMAN—Air Force Manual

AFPD—Air Force Policy Directive

CUI—Controlled Unclassified Information

DCS—Deputy Chief of Staff

DoD—Department of Defense

DoDD—Department of Defense Directive

DPO—Defense Privacy Office

DRU—Direct Reporting Unit

EITDR—Enterprise Information Technology Data Repository

FIPS—Federal Information Processing Standard

FIPPS—Fair Information Practice Principles

FOA—Field Operating Agency

FOIA—Freedom of Information Act

FOUO—For Official Use Only

HAF—Headquarters Air Force

IAM—Information Assurance Manager

IG—Inspector General

ISO—Information System Owner

IT—Information Technology

MAJCOM/HAF/FOA/DRU—Major Command

OMB—Office of Management and Budget

OPR—Office of Primary Responsibility

PA—Public Affairs

PAS—Privacy Act Statement

PIA—Privacy Impact Assessment

PL—Public Law

PM—Program Manager

SFMIS—Security Forces Management Information System

SJA—Staff Judge Advocate

SORN—System of Records Notice

SSN—Social Security Number

US—United States

USC—United States Code

USCERT—United States Computer Emergency Response Team

Terms

Access—Allowing individuals to review or receive copies of government records that contain personally identifiable information about them.

Amendment—The process of adding, deleting, or changing information in a system of records to make the data accurate, relevant, timely, or complete.

Alteration—A significant increase or change in the number or type of individuals about whom records are maintained. Increases in numbers of individuals due to normal growth are not considered alterations unless they truly alter the character and purpose of the system. Increases that change significantly the scope of population covered (for example, expansion of a system of records covering a single command's enlisted personnel to include all of the Component's enlisted personnel would be considered an alteration). A reduction in the number of individuals covered is not an alteration, but only an amendment. All changes that add new categories of individuals to system coverage require a change to the "Categories of individuals covered by the system" caption of the notice and may require changes to the "Purpose(s)" caption.

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—A computerized comparison of two or more automated systems of records or a system of records with non-Federal records to establish or verify eligibility for payments under Federal benefit programs or to recover delinquent debts for these programs.

Confidentiality—An expressed and recorded promise to withhold the identity of a source or the information provided by a source.

Controlled Unclassified Information (CUI)—Types of information that require application of controls and protective measures for a variety of reasons. This information is also known as "unclassified controlled information."

Cookie—Data created by a Web server that is stored on a user's computer either temporarily for that session only or permanently on the hard disk (***persistent cookie***). It provides a way for the Web site to identify users and keep track of their preferences. It is commonly used to "maintain the state" of the session. A ***third-party cookie*** either originates on or is sent to a Web site different from the one you are currently viewing.

Defense Data Integrity Board—Composed of representatives from DoD components and the services who oversee, coordinate, and approve all DoD computer matching programs covered by the Act.

Denial Authority—The individuals with authority to deny requests for access or amendment of records under the Privacy Act.

Disclosure—The transfer of any personally identifiable information from a system of records by any means of communication (such as oral, written, electronic, mechanical, or actual review) to any person, private entity, or Government Agency, other than the subject of the record, the subject's designated agent, or the subject's legal guardian.

For Official Use Only (FOUO)—is a designation that is applied to unclassified information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA).

Federal Benefit Program—A federally funded or administered program for individuals that provides cash or in-kind assistance (payments, grants, loans, or loan guarantees).

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).

First Party Requester—A subject or designated representative asking for access to his/her Privacy Act records. The identity of the subject requester must be verified. A notarized signature or a sworn declaration under penalty from the record subject is one method to determine identification.

Individual—Under the Privacy Act, a citizen of the United States or an alien lawfully admitted for permanent residence.

Member of the Public—Any individual or party acting in a private capacity to include Federal employees or military personnel.

Minor—Anyone under the age of majority as an adult according to local state law. The legal age of majority may be different in overseas locations. If there is no applicable state law, a minor is anyone under the age of 18 years. Military members and married persons are not minors, no matter what their chronological age.

PII—personally identifiable information; see *Personal Identifier* and *Personal Information*

Personal Identifier—A name, number, or symbol that is unique to an individual and can be used to trace an individual identity, usually the person's name or SSN.

Personal Information—Information about an individual that identifies, links, relates, or is unique to, or describes him or her, e.g., SSN; age; military rank; civilian grade; marital status; race; salary; home/office phone numbers; other demographic, biometric, personnel, medical, and financial information, etc. Such information is also known as *personally identifiable information* (PII) (i.e., information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date of birth, place of birth, mother's maiden name, or biometric records, including any other PII which is linked or linkable to a specified individual).

Privacy Act Request—A request from an individual for notification as to the existence of, access to, or amendment of records pertaining to that individual. These records must be maintained in a system of records.

Privacy Act Statement—When soliciting personal information (i.e., SSN, home address, etc.) and including in a system of record, the following information must be given to the individual:

a. **AUTHORITY**— the federal statute or executive order that authorizes the collection of the information;

b. **PRINCIPLE PURPOSE(S)**— the purpose or purposes for which the information is to be used;

c. **ROUTINE USE(S)**— how the information will be used outside of the DoD;

d. **MANDATORY OR VOLUNTARY**— if the statute or executive order provides a penalty for not providing the information, then it is mandatory.

Privacy Act System of Records—See System of Records.

Privacy Act System Notice—See System of Records Notice (SORN).

Privacy Act Complaint—An allegation that the Agency did not comply with specific provisions of the Privacy Act, 5 USC section 552a, with respect to the maintenance, amendment, or dissemination of Privacy Act records.

Privacy Act Violations:

a. When an individual or agency who knowingly and/or willingly makes a determination under the Privacy Act of 1974 paragraph (d)(3) not to amend an individual's records in accordance with his/her request, or fails to make such review in conformity with that subsection; refuses to comply with an individual request under (d)(1); fails to maintain any records concerning:

any individual with such accuracy, relevance, timeliness, and completeness as is necessary to

assure fairness in any determination to the qualifications, character, rights, or opportunities of, or

benefits to the individual that may be made on the basis of such record, and consequently a 3

determination is made which is adverse to the individual; or fails to comply with any other

provision or rule promulgated there under, in such a way as to have an adverse effect on an

individual, the individual may bring a civil action against the agency, and the district courts of

the United States shall have jurisdiction in the matters under the provisions of this subsection.

b. When an individual or agency who knowingly and/or willingly maintains a system of records without a relevant and necessary need to accomplish a purpose of the agency required to

be accomplished by statute or by executive order of the President; fails to inform each individual whom it asks to supply information, on a form which it uses to collect the information or on

a separate form that can be retained by the individual: the authority (whether granted by statute,

or by executive order of the President) which authorizes the solicitation of the information and

whether the disclosure of such information is mandatory or voluntary; the principal purpose or

purposes for which the information is intended to be used; the routine uses which may be made

of the information, as published pursuant to paragraph (4)(D) of the Privacy Act; the effects on

him/her, if any, of not providing all or any part of the requested information.

Privacy Advisory—A statement required when soliciting personally-identifying information by an Air Force web site and the information is not maintained in a system of records. The Privacy Advisory informs the individual why the information is being solicited and how it will be used.

Privacy Impact Assessment—A written assessment of an information system that addresses the information to be collected, the purpose and intended use; with whom the information will be shared; notice or opportunities for consent to individuals; how the information will be secured; and whether a new system of records is being created under the Privacy Act.

Program Manager (PM)—The individual specifically designated to be responsible for the life cycle management of a system or end item. The PM is vested with full authority, responsibility, and resources to execute and support an approved Air Force program. The PM is accountable for credible cost, schedule, and performance reporting to the Milestone Decision Authority (DoD 5000.1). Throughout this document the term "Program Manager" is used for consistency with DoD policy and documentation. Air Force organizations may use "System Program Manager" (SPM) as an equivalent to the DoD 5000.1 "PM" term. (AFI 63-101).

Routine Use—A disclosure of records to individuals or agencies outside DoD for a use that is compatible with the purpose for which the Air Force created the records.

Sensitive Information—The Computer Security Act of 1987 established requirements for protection of certain information in Federal Government automated information systems (AIS). This information is referred to as "sensitive" information, defined in the Act as: "Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy."

System Manager—The official who is responsible for managing a system of records including guidance and procedures to operate and safeguard it. Also known as the System of Records Manager. Local system managers operate record systems or are responsible for part of a decentralized system whether paper or electronic.

System Notice—See System of Records Notice (SORN).

System of Records—A group of records under the control of a DoD Component from which an individual's record is retrieved by the name or personal identifier.

System of Records Notice (abbreviated: SORN) /or/ Privacy Act System Notice—The official public notice published in the *Federal Register* of the existence, content, and Points of Contact for the system of records containing Privacy Act data.

Third Party Requester—A request from any person for access to another individual's Privacy Act record without that individual's written consent.

Attachment 2

PREPARING A SYSTEM OF RECORDS NOTICE (SORN)

A2.1. The following elements comprise a SORN for publication in the Federal Register , *(For examples see Privacy COP):* **https://afkm.wpafb.af.mil/ASPs/docman/DOCMain.asp?Tab=0&FolderID=OO-SC-AF-53-5-6&Filter=OO-SC-AF-53.**

A2.2. System Identifier. AF Privacy Office, SAF/A6PP assigns the notice number, for example, F033 AF PC A, where "F" indicates "Air Force," the next number represents the publication series number related to the subject matter, and the final letter group shows the system manager's command or Deputy Chief of Staff (DCS). The last character "A" indicates that this is the first notice for this series and system manager.

A2.3. System Name. Use a short, specific, plain-language title that identifies the system's general purpose (limited to 55 characters).

A2.4. System Location. Specify the address of the primary system and any decentralized elements, including automated data systems with a central computer facility and input or output terminals at separate locations. Use street address, 2-letter state abbreviations and 9-digit ZIP Codes. Spell out office names. Do not use office symbols.

A2.5. Categories of Individuals Covered by the System. Use nontechnical, specific categories of individuals about whom the Air Force keeps records. Do not use categories like "all Air Force personnel" unless they are actually true.

A2.6. Categories of Records in the System. Describe in clear, plain language, all categories of records in the system. List only documents actually kept in the system. Do not show source documents that are used to collect data and then destroyed. Do not list form numbers.

A2.7. Authority for Maintenance of the System. Cite the specific law or executive order, or regulation that authorizes the program the record supports. **NOTE**: Executive Order 9397 (SSN), as amended, authorizes, but does require the use of the SSN as a personal identifier. Include this authority whenever the SSN is used to retrieve records.

A2.8. Purpose. Describe briefly and specifically what the Air Force does with the information collected.

A2.9. Routine Uses of Records Maintained in the System Including Categories of Users and the Purpose of Such Uses. List each specific agency or activity outside DoD to whom the records may be released and the purpose for such release. The DoD 'Blanket Routine Uses' published in the Air Force Directory of System Notices apply to all system notices.

A2.10. Guidance for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

A2.10.1. **Storage.** State the medium in which the Air Force keeps the records; for example, in file folders, card files, microfiche, computer, or a combination of those methods. Storage does not refer to the storage container.

A2.10.2. **Retrievability**. State how the Air Force retrieves the records; for example, by name, SSN, or personal characteristics (such as fingerprints or voiceprints).

A2.10.3. **Safeguards**. List the kinds of officials who have immediate access to the system. List those responsible for safeguarding the records. Identify the system safeguards; for example, storage in safes, vaults, locked cabinets or rooms, use of guards, visitor controls, personnel screening, computer systems software, and so on. Describe safeguards fully without compromising system security.

A2.10.4. **Retention and Disposal**. State how long the activity must maintain the record IAW its approved Records Disposition. Indicate if or when the records may be transferred to a Federal Records Center and how long the record stays there. Specify when the Records Center transfers legal ownership of (accession) the record to the National Archives or when the Records center destroys the record. Indicate how the records may be destroyed. Consult with your Records Professional on finding an appropriate disposition in the AF Records Disposition Schedule in AFRIMS, **https://www.my.af.mil/afrims/afrims/afrims/rims.cfm**

A2.11. System Manager and Address. List the position title and duty address of the system manager. For decentralized systems, show the locations and the position or duty title of each category of officials responsible for any segment of the system.

A2.12. Notification Procedure. List the title and duty address of the official authorized to tell requesters if their records are in the system. Specify the information a requester must submit; for example, full name, military status, SSN, date of birth, or proof of identity, and so on.

A2.13. Record Access Procedures. Explain how individuals may arrange to access their records. Include the titles or categories of officials who may assist; for example, the system manager.

A2.14. Contesting Records Procedures. SAF/A6PPF provides this standard caption.

A2.15. Record Source Categories. Show categories of individuals or other information sources for the system.

A2.16. Exemptions Claimed for the System. When a system has no approved exemption, write "none" under this heading. Specifically list any approved exemption including the subsection in the Act.

Attachment 3

DOD BLANKET ROUTINE USE

The DOD 'BLANKET ROUTINE USES' are at http://privacy.defense.gov/blanket_uses.shtml.

A3.1. DOD Blanket Routine Uses. Certain DoD 'blanket routine uses' have been established that are applicable to every record system maintained by the Department of the Air Force, unless specifically stated otherwise within the particular record system notice. These additional routine uses of the records are published only once in the Air Force's Preamble to its compilation of records systems in the interest of simplicity, economy and to avoid redundancy.

A3.2. Law Enforcement Routine Use. If a system of records maintained by a DoD Component to carry out its functions indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or by regulation, rule, or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the agency concerned, whether federal, state, local, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto.

A3.3. Disclosure when Requesting Information Routine Use. A record from a system of records maintained by a Component may be disclosed as a routine use to a federal, state, or local agency maintaining civil, criminal, or other relevant enforcement information or other pertinent information, such as current licenses, if necessary to obtain information relevant to a Component decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit.

A3.4. Disclosure of Requested Information Routine Use. A record from a system of records maintained by a Component may be disclosed to a federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.

A3.5. Congressional Inquiries Routine Use. Disclosure from a system of records maintained by a Component may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

A3.6. Private Relief Legislation Routine Use. Relevant information contained in all systems of records of the Department of Defense published on or before August 22, 1975, will be disclosed to the Office of Management and Budget in connection with the review of private relief legislation as set forth in Office of Management and Budget Circular A-19 at any stage of the legislative coordination and clearance process as set forth in that Circular.

A3.7. Disclosures Required by International Agreements Routine Use. A record from a system of records maintained by a Component may be disclosed to foreign law enforcement, security, investigatory, or administrative authorities to comply with requirements imposed by, or to claim rights conferred in, international agreements and arrangements including those regulating the stationing and status in foreign countries of DOD military and civilian personnel.

A3.8. Disclosure to State and Local Taxing Authorities Routine Use. Any information normally contained in Internal Revenue Service (IRS) Form W-2 which is maintained in a record from a system of records maintained by a Component may be disclosed to state and local taxing authorities with which the Secretary of the Treasury has entered into agreements under 5 U.S.C., sections 5516, 5517, and 5520 and only to those state and local taxing authorities for which an employee or military member is or was subject to tax regardless of whether tax is or was withheld. This routine use is in accordance with Treasury Fiscal Requirements Manual Bulletin No. 76-07.

A3.9. Disclosure to the Office of Personnel Management Routine Use. A record from a system of records subject to the Privacy Act and maintained by a Component may be disclosed to the Office of Personnel Management (OPM) concerning information on pay and leave, benefits, retirement deduction, and any other information necessary for the OPM to carry out its legally authorized government-wide personnel management functions and studies.

A3.10. Disclosure to the Department of Justice for Litigation Routine Use. A record from a system of records maintained by this component may be disclosed as a routine use to any component of the Department of Justice for the purpose of representing the Department of Defense, or any officer, employee or member of the Department in pending or potential litigation to which the record is pertinent.

A3.11. Disclosure to Military Banking Facilities Overseas Routine Use. Information as to current military addresses and assignments may be provided to military banking facilities who provide banking services overseas and who are reimbursed by the Government for certain checking and loan losses. For personnel separated, discharged, or retired from the Armed Forces, information as to last known residential or home of record address may be provided to the military banking facility upon certification by a banking facility officer that the facility has a returned or dishonored check negotiated by the individual or the individual has defaulted on a loan and that if restitution is not made by the individual, the U.S. Government will be liable for the losses the facility may incur.

A3.12. Disclosure of Information to the General Services Administration (GSA) Routine Use. A record from a system of records maintained by this component may be disclosed as a routine use to the General Services Administration (GSA) for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

A3.13. Disclosure of Information to the National Archives and Records Administration (NARA) Routine Use. A record from a system of records maintained by this component may be disclosed as a routine use to the National Archives and Records Administration (NARA) for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

A3.14. Disclosure to the Merit Systems Protection Board Routine Use. A record from a system of records maintained by this component may be disclosed as a routine use to the Merit Systems Protection Board, including the Office of the Special Counsel for the purpose of litigation, including administrative proceedings, appeals, special studies of the civil service and other merit systems, review of OPM or component rules and regulations, investigation of alleged or possible prohibited personnel practices; including administrative proceedings involving any individual subject of a DoD investigation, and such other functions, promulgated in 5 U.S.C. 1205 and 1206, or as may be authorized by law.

A3.15. Counterintelligence Purpose Routine Use. A record from a system of records maintained by this component may be disclosed as a routine use outside the DoD or the U.S. Government for the purpose of counterintelligence activities authorized by U.S. Law or Executive Order or for the purpose of enforcing laws, which protect the national security of the United States.

Attachment 4

ALTERING A SYSTEM OF RECORD NOTICE

A4.1. A system is considered altered.

Table A4.1. Criteria for altering a system of records notice.

Alterations	DoD 5400.11-R Citation	DoD 5400.11-R Exclusions
Categories of Individuals: C6.4.2.1. A significant increase or change in the number or type of individuals about whom records are maintained.	C6.4.2.1.1. Only changes that alter significantly the character and purpose of the record system are considered alterations.	C6.4.2.1.2. Increases in numbers of individuals due to normal growth are not considered alterations unless they truly alter the character and purpose of the system.
	C6.4.2.1.3. Increases that change significantly the scope of population covered.	C6.4.2.1.4. A reduction in the number of individuals covered is not an alteration, but only an amendment.
	C6.4.2.1.5. All changes that add new categories of individuals to system coverage require a change to the "Categories of individuals covered by the system" caption of the notice	
Categories of Records: C6.4.2.2. An expansion in the types or categories of information maintained.	C6.4.2.2.3. All changes under this criterion require a change to the "Categories of Records in the System" caption of the notice.	
Retrievability: C6.4.2.3. An alteration of how the records are organized or the manner in which the records are indexed and retrieved.	C6.4.2.3.2. Any change under this criterion requires a change in the "Retrievability" caption of the system notice.	
	C6.4.2.3.3. If the records are no longer retrieved by name or personal identifier, cancel the system notice.	
Purpose: C6.4.2.4. A change in the purpose for which the information in the system is used.	C6.4.2.4.1. The new purpose must not be compatible with the existing purposes for which the system is maintained.	C6.4.2.4.2. If the use is compatible and reasonably expected, there is no change in purpose and no alteration occurs.
	C6.4.2.4.3. Any change under this criterion requires a change in the	

Alterations	DoD 5400.11-R Citation	DoD 5400.11-R Exclusions
	"Purpose(s)" caption (see paragraph C6.3.8. of this Chapter) and may require a change in the "Authority for maintenance of the system" caption (see paragraph C6.3.7. of this Chapter).	
Location:	C6.4.2.5.1. Increasing the number of offices with direct access is an alteration.	
Combining System of Records:	C6.4.2.3.1. The change must alter the nature of use or scope of the records involved (for example, combining records systems in reorganization).	
Computer Environment: C.6.4.2.5. Changes that alter the computer environment (such as, changes to equipment configuration, software, or procedures) so as to create the potential for greater or easier access	C6.4.2.5.2. Software applications, such as operating systems and system utilities, which provide for easier access, are considered alterations.	
	C6.4.2.5.3. The addition of an on-line capability to a previously batch-oriented system is an alteration.	
	C6.4.2.5.4. The addition of peripheral devices such as, tape devices, disk devices, card readers, printers, and similar devices to an existing IT system constitute an amendment if system security is preserved.	
Storage:	C6.4.2.5.6. The connecting of two or more formerly independent automated systems or networks together creating a potential for greater access is an alteration.	
	C6.4.2.5.7. Any change under this caption requires a change to the "Storage" caption element of the systems notice.	

Attachment 5

RISK ASSESSMENT

A5.1. Risk Notification. Five factors are used when determining if an agency is required to notify those who may have been affected by a PII breach. Agencies should take the time to determine the risk of harm surrounding the breach. The factors used in assessing the likely risk of harm are

A5.1.1. **Nature of Data Elements Breached.** Consider context of the data involved and the potential harm that might be generated by its exposure to unauthorized individuals.

A5.1.2. **Number of Individuals Affected.** The magnitude of the number of individuals affected may determine how they will be notified, but should not impact an agency's decision to provide notification.

A5.1.3. **Likelihood the Information is Accessible and Useable.** Upon discovery of a breach, agencies should assess the likelihood the personally identifiable information has been or will be used by unauthorized individuals. Increased risk the information will be used should influence an agency's decision to provide notification.

A5.1.4. Likelihood the Breach May Lead to Harm.

A5.1.4.1. **Broad Reach of Potential Harm.** Consider the possible harm associated with the loss or compromise of the PII, i.e., loss of self esteem, mental pain or emotional stress.

A5.1.4.2. **Likelihood Harm Will Occur.** Agencies must determine the type of data has been compromised and the manner the breach occurred.

A5.1.5. **Ability of the Agencies to Mitigate the Risk of Harm.** In addition to containing the breach, agencies must determine what countermeasures will be used to prevent further compromise of the system's PII.

Table A5.1. Portrays the Risk Assessment Model referenced by the June 2009 DoD Policy Memo, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII).*

No.	Factor	Risk Determination	Low Moderate High	**Comments:** All breaches of PII, whether actual or suspected, require notification to US-CERT. **Low** and **Moderate** risk/harm determinations and the decision whether notification of individuals is made; rest with the Head of DoD Component where the breach occurred. **All determinations of High risk or harm require notification**
1	What is the nature of the data elements breached? What PII was involved??			
	a. Name only	Low		Consideration needs to be given to unique names; those where one or only a few in the population may have or those who could readily identify an individual, i.e. public figure

	b. Name plus 1 or more personal identifier (not SSN, Medical or Financial)	Moderate		Additional identifiers include date and place of birth, mother's maiden name, biometric record, and any other information that can be linked or is linkable to an individual
	c. SSN	High		
	d. Name plus SSN	High		
	e. Name plus Medical or Financial data	High		
2	Number of individuals Affected			The number of individuals involved is a determining factor in how notifications are made, not whether they are made
3	What is the likelihood the information is accessible and usable? What level of p-protection applied to this information?			
	a. Encryption (FIPS 140-2)	Low		
	b. Password	Moderate/High		Moderate/High determined in relationship to category of data in No. 1
	c. None	High		
4	Likelihood the Breach May Lead to Harm	High/Moderate/Low		Determining likelihood depends on the manner of the breach and the type(s) of data involved
5	Ability of the Agency to Mitigate the Risk of Harm			
	a. Loss	High		Evidence exists that PII has been stolen and could possibly be used to commit theft?
	b. Theft	High		Evidence shows that PII has been stolen and could possibly be used to commit ID theft?
	c. Compromise			
	(1) Compromise w/I DoD control	Low/High		No evidence of malicious intent. Evidence or possibility of malicious intent
	(2) Compromise beyond DoD control	High		Possibility that PII could be used with malicious intent or to commit ID theft

Attachment 6

PREPARING A DOD SSN JUSTIFICATION MEMORANDUM

(Month, Day, Year)
MEMORANDUM THRU
FOR

SUBJECT: Justification for the Use of the Social Security Number (SSN)

The memorandum should begin by naming and describing the system or form that is the subject of the justification. The description is sufficiently detailed so that someone unfamiliar with the system is should be able to grasp a general understanding of its intent.

The justification for the use of the SSN must include a reference to the SSN Instruction Use Case that is being used to justify the use of the SSN. If the justification does not fall under either the operational necessity use case or the legacy system interface use case, then the justification shall also include the specific reference to the law that requires the use of the SSN and why it is applicable to the use being justified.

Reference is made to the system or form supporting documentation, including but not limited to, System of Records Notice (SORN), Privacy Impact Assessment (PIA), Paperwork Reduction Act (PRA) notice, or any other documentation that may be appropriate. If the substance of the documentation is not attached, reference is made to how the reader may gain access to this documentation.

Justification for the use of the SSN does not constitute blanket permission to use the SSN. Specific reference shall be made to indicate actions being taken to reduce the vulnerability of SSNs, which may include indicating where SSNs are being removed from transactions, where SSNs are no longer displayed, or any other protections that have been included. It should be obvious to the reader that a thorough effort has been made to evaluate the risk associated with the system or form and that every reasonable step has been or is being taken to reduce the use of the SSN and protect it where the use is still required.

If the justification for the use of the SSN falls under the “legacy use” authorization and is not specifically required by the law, reference shall be made to the Plan of Actions and Milestones for the elimination of the use of the SSN.

Official’s Name
Title

Attachment 7

EXAMPLE PRIVACY BREACH NOTIFICATION LETTER

OFFICIAL LETTERHEAD

Dear Mr. John Miller:
On January 1, 2006, a DoD laptop computer was stolen from the parked car of a DoD employee in Washington, D.C. after normal duty hours while the employee was running a personal errand. The laptop contained personally identifying information on 100 DoD employees who were participating in the xxx Program. The compromised information is the name, social security number, residential address, date of birth, office and home email address, office, and home telephone numbers of the Program participants.

The theft was immediately reported to local and DoD law enforcement authorities, who are now conducting a joint inquiry into the loss.

We believe that the laptop was the target of the theft as opposed to any information that the laptop might contain. Because the information in the laptop was password protected and encrypted, we also believe that the probability is low that the information will be acquired and used for an unlawful purpose. However, we cannot say with certainty that this might not occur. We therefore believe that you should consider taking such actions to protect against the potential that someone might use the information to steal your identity.

You should be guided by the actions recommended by the Federal Trade Commission (FTC) on its Web site at http://www.ftc.gov/bcp/edu/microsites/idtheft/ . The FTC urges that you to immediately place an initial fraud alert on your credit file. The fraud alert is for a period of 90 days, during which, creditors are required to contact you before a new credit card is issued or an existing card changed. The site also provides other valuable information that can be taken now or in the future if problems should develop.

The Department of Defense takes this loss very seriously and is reviewing its current policies and practices with a view of determining what must be changed to preclude a similar occurrence in the future. At a minimum, we will be providing additional training to personnel to ensure that they understand that personally identifiable information must at all times be treated in a manner that preserves and protects the confidentiality of the data.

We deeply regret and apologize for any inconvenience and concern this theft may cause you.

Should you have any questions, please call _____.

Sincerely,
Signature Block
(Directorate level or higher)