BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-332

10 MARCH 2020

Communication and Information

AIR FORCE PRIVACY AND CIVIL LIBERTIES 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 or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: SAF/CNZA

Certified by: SAF/CNZ
(Ms. Wanda Jones-Heath)

Supersedes: AFI33-332, 12 January 2015

Pages: 61

This instruction implements Air Force Policy Directive (AFPD) 33-3, *Information Management*. This instruction applies to all Regular Air Force, Air Force Reserve, Air National Guard, civilian employees, contractors in the performance of their duties to an Air Force contract, and the Civil Air Patrol when performing functions for the Air Force. Failure to observe the prohibitions and mandatory provisions in **paragraphs 3.1.2** and **4.2.12.4**, of this publication by military members is a violation of Article 92 of the Uniform Code of Military Justice (UCMJ). Air National Guard members not serving in a federal status who violate the mandatory provisions in **paragraphs 3.1.2** and **4.2.12.4** may be punished under their respective state military codes or applicable administrative action may be taken, as appropriate. Personnel not in a federal status are subject to their respective state military code or applicable administrative actions, as appropriate. Civilians who violate information security policy may be disciplined in accordance with AFI 36-704, *Discipline and Adverse Actions of Civilian Employees* or AFI 34-301, *Nonappropriated Funds Personnel Management and Administration*. In addition to this instruction, Air Force medical organizations that meet the definition of a covered entity must also comply with DoDI 6025.18, *Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule Compliance In DoD Health Care Programs*, DoDI 8580.02, *Security of Individually Identifiable Health Information in DoD Health Care Programs;* and Air Force Manual (AFMAN) 41-210, *TRICARE Operations and Patient Administration*, which covers Protected Health Information (PHI) held by them. The authorities to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See AFI 33-360, *Publications and Forms Management*, for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval

authority, or alternately, to the requestor's commander for non-tiered compliance items. Ensure all records generated as a result of processes prescribed in this publication adhere to Air Force Instruction 33-322, *Records Management and Information Governance Program* and are disposed in accordance with the Air Force Records Disposition Schedule which is located in the Air Force Records Information Management System. Use of the term "Major Command" (MAJCOM) throughout this AFI includes Headquarters AF (HAF), MAJCOMs, Field Operating Agencies (FOAs), Direct Reporting Units (DRUs), and the Air Force Installation Mission Support Center (AFIMSC). Refer recommended changes and questions about this instruction to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route through the appropriate functional chain of command. Send supplements and implementing publications of this instruction to the Deputy Chief Information Officer, Compliance Division (SAF/CNZA), 1800 Air Force Pentagon, Washington, DC 20330-1800 for review and coordination prior to publication. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force. This instruction includes reference to trade name and trademarks such as SharePoint®.

SUMMARY OF CHANGES

This document has been substantially revised and needs to be completely reviewed. Major changes include revising guidance to comply with the E-Government Act of 2002, Office of Management and Budget Circulars No. A-130, *Managing Information as a Strategic Resource* and A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act* and Office of Management and Budget Memorandum Circular No. 17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*.

Chapter 1

PRIVACY OVERVIEW

1.1. Privacy Overview.

1.1.1. What is privacy? Although there is not an official government definition of privacy, it generally refers to the notion of individuals maintaining control over their own information. For the Air Force, the framework of privacy requirements includes the *Privacy Act of 1974,* Title 5 United States Code (USC) Section 552a, Public Law 107-347, Section 208, *The E-Government Act of 2002,* Office of Management and Budget policy, Department of Defense (DoD) policy, and Air Force policy. Failure to protect privacy can bring about risks to the individual, such as identity theft, and risks to the Air Force, such as lawsuits for inappropriate disclosure that divert critical resources away from our mission.

1.1.2. What information must be protected? The information protected by the various components of the privacy framework is discussed using multiple terms.

1.2. Civil Liberties Overview.

1.2.1. Civil liberties are fundamental rights and freedoms protected by The Constitution of the United States. These freedoms, which include the right to privacy, are concentrated primarily in the Bill of Rights.

1.2.2. Individuals who feel any of the following provided examples (the list is not exhaustive) has been violated shall seek direction through their servicing Inspector General office; (See AFI 90-301, *Inspector General Complaints Resolution*).

1.3. Personally Identifiable Information (PII).

1.3.1. Office of Management and Budget Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* – "The term PII refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. PII may range from common data elements such as names, addresses, dates of birth, and places of employment, to identity documents, Social Security numbers (SSN) or other government-issued identity, precise location information, medical history, and biometrics. Because there are many different types of information that can be used to distinguish or trace an individual's identity the term PII is necessarily broad..

1.3.2. Office of Management and Budget Memorandum 10-22, *Guidance for Online Use of Web Measurement and Customization Technologies* - The definition of PII is not anchored to any single category of information or technology. Rather, it demands a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available – in any medium and from any source – that, when combined with other available information, could be used to identify an individual.

1.3.3. For safeguarding of Personal Identifiable Information, please refer to DoD 5400.11-R, *Department of Defense Privacy Program* (C1.4, C4 and Appendix 1).

1.3.4. PII maintained in a System of Record accessed or handled by contractors. It is imperative that contractors, required to access or handle PII on behalf of the Air Force, follow this instruction. For this reason, organizations with contractors that access and handle PII will coordinate with contracting officials to ensure that contract require compliance with this instruction. **(T-1).** Additionally, organizations will coordinate with contracting officers to ensure contracts contain the proper Privacy Act clauses: 52.224-1, Privacy Act Notification, and 52.224-2, Privacy Act as required by the Federal Acquisition Regulation (See website at: **https://www.acquisition.gov/browse/index/far** .) Contracting Officers will also require non-disclosure agreements for contractors who will have access to sensitive PII. **(T-0). Note**: All contracts either need the Network Penetration or Cloud DFAR clauses to comply with the requirements for contractors protecting PII in OMB Memo 17-12.

1.3.5. Contracts will be reviewed annually by the Contracting Officer Representative to ensure compliance with this instruction. **(T-0).**

1.3.6. Disclosure of PII maintained in a System of Records to contractors 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 and protected as an inter/intra-Agency disclosure per Freedom of Information Act exemption (b)(5).

Chapter 2

ROLES AND RESPONSIBILITIES

2.1. The Deputy Chief Information Officer (SAF/CN) shall:

2.1.1. Establish procedures to ensure compliance with the Privacy Act and the DoD privacy program. **(T-0).**

2.1.2. Appoint a Senior Component Official for Privacy (SCOP) with overall responsibility for the AF privacy program. **(T-0).**

2.1.3. Appoint an AF Privacy Officer with responsibility for implementing the AF privacy program. **(T-0).**

2.2. SAF/IG and AF/A1 shall:

2.2.1. Coordinate with SAF/GC and AF/JA on any Privacy or Civil Liberty matter, review, or investigation, that does any of the following: affect or involve the Secretariat; represent a significant litigation risk; impact major AF programs; materially impact the rights or benefits of an AF organization; affect ownership or use of AF property; attract Congressional interest; attract widespread media interest; raise a matter of first impression for the legal community; or otherwise affect the legal basis for an AF program or activity. **(T-0).**

2.2.2. Identify and report Civil Liberties complaint allegations received and processed by Inspector General or Equal Employment Opportunity and Military Equal Opportunity offices on a semi-annual basis. **(T-1).**

2.2.3. Submit complaint(s) with Civil Liberties implications to the AF Civil Liberties POC using the DD Form 2984, *Component Privacy and Civil Liberties Report*. (See **Attachment 9**). Reports are forwarded directly by unencrypted e-mail without identifying PII to the AF Privacy and Civil Liberties workflow e-mail at **usaf.pentagon.saf-cn.mbx.af-privacy@mail.mil**. **(T-1).**

2.2.4. Provide Civil Liberties reporting requirements to the MAJCOM IG offices. **(T-1).**

2.3. The Senior Component Official for Privacy (SCOP) shall:

2.3.1. Ensure DoD and AF proposals, policies, or programs having privacy implications are evaluated to ensure consistency with privacy principles. **(T-0).**

2.3.2. Ensure the AF privacy program is periodically reviewed by the Inspector General or other officials who have specialized knowledge of the privacy policies. **(T-0).**

2.3.3. Supervise and oversee management of the AF Privacy Program as administered by the AF Privacy Officer. **(T-0).**

2.3.4. The SCOP or the AF Privacy Officer will serve as the AF representative on the Defense Privacy Board and the Defense Data Integrity Board, which are administered through the Defense Privacy, Civil Liberties, and Transparency Division. **(T-0).**

2.3.5. Designated as the AF Civil Liberties Officer. **(T-0).**

2.3.6. Oversee the AF Civil Liberties program with execution by the AF Civil Liberties point of contact (POC). **(T-0).**

2.3.7. Review and approve AF Civil Liberties reports prior to submission to Defense Privacy, Civil Liberties, and Transparency Division. **(T-0).**

2.4. The AF Privacy Officer shall:

2.4.1. Administer guidance and procedures prescribed in this instruction and DoD policies, develop Air Force policy to ensure protection of PII, and provide guidance and assistance to Privacy Managers. **(T-1).**

2.4.2. Conduct mandatory reviews of publications and forms for compliance with this instruction. **(T-1).**

2.4.3. Review and approve Privacy Impact Assessments (PIA) for submission to SAF/CN for approval (see **paragraph 5.2**). **(T-1)**

2.4.4. Review and submit proposed new, modified, and deleted System of Records Notice (SORN) to Defense Privacy, Civil Liberties, and Transparency Division. **(T-1).**

2.4.5. Review and approve SSN justification memos for continued use of SSN. **(T-1).**

2.4.6. Report Privacy Breaches to the Defense Privacy, Civil Liberties, and Transparency Division within the prescribed timelines and track and monitor breach trends to improve guidance and procedures. **(T-1).**

2.4.7. Prepare and submit reports as required to Defense Privacy, Civil Liberties, and Transparency Division. **(T-1).**

2.4.8. Provide guidance and support to the field to ensure information systems which are developed to collect, maintain, process, or disseminate personal information conform to the Privacy Act, Office of Management and Budget, DoD, and AF requirements. **(T-1).**

2.4.9. Coordinate with SAF/CNZ, Information System Security Office, to ensure appropriate Information Assurance (IA) Control procedures are applied by Information System Owners, Program/Project Managers and Portfolio Managers during the Certification and Accreditation (C&A) process to protect Privacy Act information throughout the IT system life cycle. **(T-1).**

2.4.10. Serve as the AF representative on the Defense Privacy Board and the Defense Data Integrity Board, which are administered through the Defense Privacy, Civil Liberties and Transparency Division. **(T-1).**

2.4.11. Designated as the AF Civil Liberties POC. **(T-1).**

2.4.12. Serve as the AF member on the Defense Civil Liberties board. **(T-1).**

2.4.13. Provide policy and direction for the AF Civil Liberties program. **(T-1).**

2.4.14. Review AF publications and policies to support the proper protection of Civil Liberties. **(T-1).**

2.4.15. Compile and submit the AF semi-annual Civil Liberties report to the Defense Privacy and Civil Liberties Office. **(T-1).**

2.4.16. Provide Secretary of the Air Force (SAF)/General Counsel (GC) and AF/JA with copies of the AF semi-annual Civil Liberties report for situational awareness. **(T-1).**

2.4.17. Provide training and training materials to MAJCOM Privacy and Civil Liberties points of contact (POC). **(T-1).**

2.4.18. Approve the computer matching request. **(T-1).**

2.5. The Office of The Judge Advocate General (AF/JA).

2.5.1. AF/JA, primarily through the Administrative Law Directorate (AF/JAA) and the Air Force Legal Operations Agency Civil Law and Litigation Directorate (AFLOA/JAC) shall:

2.5.1.1. Provide legal advice on Civil Liberties and Privacy matters to the Department of the Air Force Staff, AF Civil Liberties Officer, Privacy Officer/Civil Liberties POC**. (T-1).**

2.5.1.2. Provide Civil Liberties reporting requirements to MAJCOM Equal Opportunity offices. **(T-1).**

2.5.1.3. Review Civil Liberties semi-annual Reports for legal sufficiency. **(T-1).**

2.5.1.4. Provide lead litigation support as necessary. **(T-1).**

2.5.1.5. Coordinate with SAF/GC as appropriate. **(T-1).**

2.5.2. Nothing in **paragraph 2.5** or its subparagraphs is inconsistent with Headquarters Air Force Mission Directive (HAFMD) 1-14, *General Counsel and The Judge Advocate General*.

2.6. Assistant Secretary of the Air Force, General Counsel of the Air Force (SAF/GC).

2.6.1. SAF/GC shall:

2.6.1.1. Provide coordination on any Civil Liberty matters, reviews, investigations, or legal opinions that represent a significant litigation risk, impact major AF programs, materially impact the rights or benefits of an AF organization, effect ownership or use of AF property, engender Congressional interest, attract widespread media interest, raise a matter of first impression for the legal community, or otherwise affect the legal basis for an AF program or activity. **(T-1).**

2.6.1.2. Coordinate with AF/JA as appropriate. **(T-1).**

2.6.2. Nothing in this paragraph is inconsistent with Headquarters Air Force Mission Directive (HAFMD) 1-14, *General Counsel and The Judge Advocate General*. **(T-1).**

2.7. AF Departmental Forms Management Officer shall:

2.7.1. Maintain 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 Federal Information Security Management Act (FISMA) report as required by Title 44 United States Code Chapter 35, Subchapter III, *Confidential Information Protection and Statistical Efficiency*. **(T-1).**

2.7.2. Ensure OPRs for new and revised forms that collect personal information have the appropriate notice as required in this instruction. Coordination is made with the supporting Privacy Manager/Monitor before publishing. Final publishing packages must contain a completed AF Form 673, *Air Force Publication/Form Action Request* in accordance with AFI 33-360; and if applicable, the associated SORN and AF Privacy Officer approved SSN justification memo. **(T-0).**

2.8. MAJCOM and Wing Commanders shall:

2.8.1. Establish a Privacy and Civil Liberties Office(s) and appoint in writing, a command Privacy Manager/Monitor to execute command responsibilities as outlined in this instruction. The same will apply at installation-level where the Wing Commander will appoint an installation Privacy Manager/Monitor and Civil Liberties POC and report to their respective command. **(T-1).**

2.8.2. Establish policies to notify MAJCOM/Wing Commanders of Privacy Act Violations, complaints and breaches. **(T-1.**

2.8.3. Establish policies to implement and enforce the AF Privacy and Civil Liberties Programs to include directing organization SharePoint® site owners or Site Collection Administrators to perform a monthly scan of SharePoint® sites. If unprotected PII data is discovered during the scan then delete and/or safeguard PII and submit a collective PII breach report (Department of Defense Form 2959). **(T-1).**

2.8.4. Ensure all assigned AF personnel are aware of and understand the requirements within this publication. **(T-1).**

2.8.5. Ensure all privacy and civil liberties related issues or concerns are brought to the attention of servicing Privacy Manager/Monitor, Civil Liberties POC or the AF Privacy Officer. **(T-0).**

2.8.6. Ensure all assigned personnel have completed required mandatory annual privacy training;

2.8.6.1. Annual Training is required by statute for all federal employees (civilian, military and contractor), DISA Identifying and Safeguarding Personally Identifiable Information refresher training, **https://public.cyber.mil/** **(T-0)**.

2.8.6.2. Specialized Training. Training that focuses on the requirements in accordance with the Privacy Act of 1974 for individuals who will maintain a System of Records (SORs). **(T-0).**

2.8.6.3. Newcomers Orientation Training is provided to newly assigned personnel which places focus on the basic requirements of the Privacy Act and Safeguarding PII. **(T-0).**

2.8.6.4. Management Training. Training that provides managers and decision makers considerations that they should take into account when making management decisions regarding actions under this chapter. **(T-0).**

2.8.6.5. Remedial training for individuals who committed a breach. **(T-0).**

2.8.7. Privacy Act Training Tools. Helpful resources include:

2.8.7.1. The Privacy Act web page includes a Privacy Overview, Privacy Act training, Resources, AF SORNs, and links to the Defense Privacy Board Advisory Opinions, the DoD and Department of Justice Privacy web pages. Go to **https://www.privacy.af.mil/**.

2.8.7.2. "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".

2.8.7.3. Training slides for use by Privacy Managers/Monitors are available in the "Information Access SharePoint® Site." **https://cs2.eis.af.mil/sites/10440/infoacc/privacy/forms/allitems.aspx**.

2.8.7.4. DISA web based training "Identifying and Safeguarding Personally Identifiable Information (PII)," **https://public.cyber.mil/**.

2.8.8. Ensure organizational Commanders and Equivalents have (examples of commander equivalents include MAJCOM Director, Director of Staff, Civilian Director of an organization, or a Commandant of a school).

2.8.8.1. Reinforce the importance of safeguarding PII and ensure personnel who fail to safeguard PII are counseled or disciplined as appropriate. **(T-0).**

2.8.8.2. Direct an inquiry to determine the circumstances and impact of privacy breaches in accordance with **Chapter 3** of this instruction. **(T-0).**

2.8.8.3. Ensure coordination and teamwork is accomplished between Information System Owner (ISO), Program (PM), Information System Security Manager (ISSM), Information System Security Officer (ISSO), and Privacy Managers. (**T-0).**

2.8.8.4. Ensure assigned personnel are aware of and understand the requirements within this instruction. **(T-1).**

2.8.8.5. Ensure additional privacy training is incorporated into in-house training, as needed. **(T-0).**

2.9. MAJCOM and Base Privacy Managers/Monitors shall:

2.9.1. Provide direction and training to commanders and personnel implementing this instruction. **(T-1).**

2.9.2. Track assigned personnel privacy training. **(T-1).**

2.9.3. Provide specialized training to individuals who handle privacy information on a daily or routine basis. **(T-1).**

2.9.4. Promote privacy awareness throughout the organization and assist commanders with establishing procedures to reinforce the protection of personal information or PII. **(T-1).**

2.9.5. Report privacy breaches and provide direction to organizations where the breach occurred. **(T-1).**

2.9.6. Provide direction to assist with resolution of Privacy Act complaints or violations. **(T-1).**

2.9.7. Review and process Privacy Act Request denial recommendations. **(T-1).**

2.9.8. Review all publications and forms drafted by staff OPRs for compliance with this instruction. (**Note:** Publications drafted for a higher level should be reviewed by the Privacy Manager at the level of the OPR. Review organizational publications and forms for compliance with this instruction.) **(T-1).**

2.9.9. Provide updates of Privacy Managers name, office symbol, phone number, FAX number, unclassified e-mail address to the Privacy Manager in their chain of command who in turn shall forward a copy to the AF Privacy Officer for continuity. **(T-1).**

2.9.10. Submit semi-annual privacy reports and/or other required reports as directed by the AF Privacy Officer. Semi-annual privacy reports may consist of the number of SORNs reviewed, privacy complaints, and training provided; complaints will be categorized as follows:

2.9.10.1. Process and Procedural: For actions concerning consent, collection, and appropriate notice **(T-1)**.

2.9.10.2. Redress: Privacy Act inquiries seeking resolution of difficulties or concerns about Privacy matters. **(T-1).**

2.9.10.3. Operational: Inquiries regarding Privacy Act matters not including Privacy Act requests for access and/or correction. **(T-1).**

2.9.10.4. Referrals: Complaints received but referred to another office with jurisdiction over the complaint. **(T-1).**

2.9.11. Conduct Staff Assistance Visits (SAVs)/Command Unit Inspections if budget permits to ensure compliance and health of privacy programs. **(T-1).**

2.9.12. Base Privacy Managers provide direction to ISO, ISSM/ISSO, and Program Manager/Project Manager for properly completing a SORN or PIA (to include signing off on the DD 2930). **(T-1).**

2.9.13. Assist ISO/Program Manager/Project Manager with reviewing SORNs and PIAs to coincide with their IT system review cycles. Coordination and teamwork are required between ISO, ISSM/ISSO, Program Manager/Project Manager and Privacy Manager. **(T-1).**

2.9.14. Maintain copies of approved inventories of records (formerly known as file plans) with System of Records for the purpose of identifying records protected under the Privacy Act of 1974 to assist with inspections. **(T-1).**

2.9.15. Address all privacy and civil liberties complaints, issues or concerns with leadership and the Air Force Privacy Officer/Civil Liberties POC. **(T-1).**

2.9.16. Monitor/Track Annual SORNs Review. **(T-1).**

2.9.17. Monitor/Track Annual PIA Review. **(T-1).**

2.10. MAJCOM and base legal offices shall:

2.10.1. On a semi-annual basis, identify and report Civil Liberties complaint allegations addressed in Commander Directed Investigation reports and Article 138 complaints that have been reviewed for legal sufficiency. **(T-0).**

2.10.2. Submit Civil Liberties complaints contained in the Commander Directed Investigations and Article 138 complaints to the Civil Liberties POC, through AF/JAA, using the DD Form 2984. (See **Attachment 9**). Reports are forwarded by unencrypted e-mail without identifying PII. **(T-0).**

2.10.3. Provide advice to the Civil Liberties POCs. **(T-1).**

2.10.4. Provide advice to the Privacy Officer/Manager/Monitor, commanders, and supervisors on requests made under the Privacy Act, the Freedom of Information Act, PII breaches, and other aspects of the AF Privacy and Civil Liberties program.

2.11. MAJCOM and base Civil Liberties POCs shall:

2.11.1. Administer direction and procedures prescribed in this instruction. **(T-1).**

2.11.2. Ensure training is available for their organizations. **(T-1).**

2.11.3. Provide updates regarding the Civil Liberties POCs' names, office symbols, voice number, and unclassified e-mail addresses to the AF Civil Liberties POC. **(T-1).**

2.11.4. Promote Civil Liberties awareness throughout their organizations. **(T-1).**

2.11.5. Direct complaints that may have Civil Liberties implications to the appropriate investigative office, such as the IG, Equal Opportunity, or the appropriate commanding officer for commander directed investigations. **(T-0).**

2.12. Unit Privacy Monitor shall:

2.12.1. Provide direction and training to commanders and personnel implementing this instruction. **(T-1).**

2.12.2. Promote privacy awareness throughout the organization and assist commanders/equivalent with implementing procedures to reinforce the protection of PII. **(T-1).**

2.12.3. Track assigned personnel privacy training. **(T-1).**

2.12.4. Provide specialized training to individuals who handle personal information or PII on a daily or routine basis. **(T-1).**

2.12.5. Review organizational publications and forms for privacy compliance with this instruction. **(T-1).**

2.12.6. Provide direction to the commander/equivalent to assist with resolution of privacy breaches, complaints, and violations. **(T-1).**

2.12.7. Submit semi-annual reports and/or other required reports as directed by their respective privacy manager. Semi-annual reports will consist of the number of SORNs reviewed, privacy complaints, and training provided; complaints should be categorized as follows:

2.12.7.1. Process and Procedural: For actions concerning consent, collection, and appropriate notice. **(T-1).**

2.12.7.2. Redress: Privacy Act inquiries seeking resolution of difficulties or concerns about Privacy matters. **(T-1).**

2.12.7.3. Operational: Inquiries regarding Privacy Act matters not including Privacy Act requests for access and/or correction. **(T-1).**

2.12.7.4. Referrals: Complaints received but referred to another office with jurisdiction over the complaint. **(T-1).**

2.12.8. Maintain copies of approved inventories of records (formerly known as file plans) with the System of Records for the purpose of identifying records protected under the Privacy Act of 1974 to assist with conducting inspections or Privacy Act request. **(T-1).**

2.13. Functional Level Information System Owner (ISO), Program Manager/Project Manager (PM), Information System Security Managers (ISSM) shall:

2.13.1. Implement privacy safeguards, complete PIAs and SORNs. Direction will be provided by supporting Privacy Manager (See **Chapters 3** and **4** and DoDI 5400.16, *DoD Privacy Impact Assessment (PIA) Guidance*). **(T-0).**

2.13.2. Determine early in the design phase of IT systems what personal information will be collected, used, processed, stored, or disseminated in the electronic systems of records. **(T-0).**

2.13.3. Formulate Privacy Act requirements in early stages of IT systems design, development, and data management to plan for and implement Information Assurance (IA) controls to safeguard PII. **(T-0).**

2.13.4. Ensure records containing PII are safeguarded or removed as required from all IT systems prior to disposal, replacement, or reuse of IT hardware storage components (hard drives) in accordance with IA directives. **(T-0).**

2.13.5. Review applicable SORN(s) for information systems concurrently with the FISMA annual review to validate whether changes to an existing SORN is required. **(T-0).**

2.13.6. Review IT systems registered in the Information Technology Investment Portfolio Suite, addresses and updates responses to privacy questions. Failure to do so may risk system non-concurrence by the AF Privacy Officer during annual compliance review, certification, decertification, or request for funding. **(T-0).**

2.13.7. The ISO is responsible for calculating the PII Confidentiality Impact Level (PCIL) value with the MAJCOM Privacy Officer's concurrence for all IT investments handling PII. In cases of disagreement, the MAJCOM Privacy Officer or ISO may raise the PCIL determination to the AF Privacy Officer for review and final determination. Documentation of the PCIL calculation may be requested upon elevation. See **paragraph 5.2.3.4** for a sample PCIL calculation worksheet. **(T-0).**

2.14. Records Professionals shall: Coordinate with Privacy Managers/Monitors to ensure records identified on inventories of records (formerly known as file plans) as a System of Records have an approved SORN. **(T-0).**

Chapter 3

BREACH REPORTING

3.1. PII Breach Reporting. Refer to Office of Management and Budget (OMB) Memorandum 17-12 *(3 January 2017), Preparing for and Responding to a Breach of Personally Identifiable Information, Office of the Secretary of Defense Memorandum (2 August 2012), Use of Best Judgement for Individual Personally Identifiable Information (PII) Breach Notification Determinations, Office of the Secretary of Defense Memorandum (OSD 06227-09, dated 5 June 2009), Safeguarding Against and Responding to the Breach of Personally Identifiable Information* **(T-0)**.

3.1.1. Per OMB Memorandum 17-12, "A PII breach is defined as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose."

3.1.2. Potential or actual breaches must be reported to the servicing Privacy Manager/Monitor by anyone discovering it. Failure by military members to obey the mandatory provision is this paragraph is a violation of Article 92(1) of the UCMJ. **(T-0).** Civilians who violate information security policy may be disciplined in accordance with AFI 36-704, *Discipline and Adverse Actions of Civilian Employees*. **(T-0).**

3.1.3. AFIMSC must provide immediate notice to the servicing Base Privacy Manager for any breaches reported from Air Force Cyber, 68th Network Warfare Squadron. **(T-1).**

3.1.4. The servicing Privacy Manager/Monitor shall submit a Preliminary PII Breach Report by unencrypted e-mail according to the timeline below: **(T-1).**

3.1.5. PII Breach Reports shall be completed using Department of Defense Form 2959, *Breach of Personally Identifiable Information (PII) Report* provided by Defense Privacy and Civil Liberties Office located on the AF Privacy Website: **www.privacy.af.mil** **(T-0)**.

3.1.6. Use for preliminary, updates, and final reports.

3.1.6.1. Reports shall not include names of individuals involved or affected by the breach. Reports will be forward by unencrypted e-mail through the serving MAJCOM Privacy Manager, who in turn shall notify the AF Privacy Office by official unencrypted e-mail (**usaf.pentagon.saf-cn.mbx.af-privacy@mail.mil**) attaching the written Preliminary PII Breach Report. **(T-0).**

3.1.6.2. Notify the United States Computer Emergency Readiness Team within one hour of discovering that an electronic breach of personally identifiable information has occurred. **(T-0).**

3.1.6.3. The Wing Commander shall submit an initial Operational Report if it is determined the breach may have an impact on organizational operations, potential media attention and affects more than 5,000 individuals. **(T-1).**

3.1.6.4. Within 24 hours of the notification of a PII breach, the servicing Privacy Manager where the incident occurred shall notify the senior official (O6/GS-15, or higher) in the

chain of command and simultaneously notify the MAJCOM Privacy Manager by official unencrypted e-mail (Non-Classified Internet Protocol Router Network) attaching the Preliminary PII Breach Report. **(T-1).**

3.1.6.5. Within 24 hours of being notified of the PII breach, the MAJCOM Privacy Manager shall notify the AF Privacy Office by official unencrypted e-mail (**usaf.pentagon.saf-cn.mbx.af-privacy@mail.mil**) attaching the written Preliminary PII Breach Report. **(T-1).**

3.1.6.6. Within 48 hours of the PII breach notification the AF Privacy Officer shall upload the report into the Defense Privacy, Civil Liberties and Transparency Division Reporting Management Tool. **(T-0).**

3.1.6.7. Until resolved, the underlying issues that led to the breach shall continue to be reported as needed in an Update PII Breach Report by the serving Privacy Manager/Monitor to the AF Privacy Office in accordance these reporting procedures. **(T-0).**

3.1.6.8. The servicing Privacy Manager shall send the PII Breach Final Report when resolved in the same routing as previous notifications along with a final operational report (if applicable). **(T-0).**

3.2. Guidelines for conducting an inquiry of a PII Incident. The senior-level individual who is in the chain of command shall appoint an investigating official (recommend E-7 or above or equivalent civilian employee) for the organization where the actual or possible loss, theft or compromise of information occurred to conduct an inquiry of the incident to determine if it is an actual breach, the cause and if a there was any criminal intent that would warrant a criminal investigation. **(T-1).**

3.2.1. The servicing Privacy Manager or Privacy Monitor shall provide guidance to the appointed investigating official to properly complete the Final PII Breach Report and reference AFI and DoD Policies and the Privacy Act for use in completing the inquiry as required. **(T-1).**

3.2.2. The appointed investigating official shall review the initial Preliminary PII Breach Report and independently assess the handling of the breach. They shall make clarifications and additions on the Final PII Breach Report as required, and submit to the appointing senior-level individual. The senior-level individual will determine if notification to affected individuals is required after a risk analysis has been completed. The senior-level individual will also determine if any corrective actions should be taken. **(T-0).**

3.2.3. Upon concurrence with Final PII Breach Report recommendations, the senior-level individual in the chain of command for the organization where the loss, theft or compromise occurred shall route the Final PII Breach Report to the appropriate level Privacy Manager within five days. **(T-1).**

3.2.4. Commanders/Directors shall ensure notifications are sent to individuals once a decision has been made as to whether there may be any impact towards the individual(s). Notification will be sent to affected individual(s) within 10 working days after a breach is confirmed and the identities of the affected individual(s) ascertained by a senior official (O6/GS-15 and higher) in the chain of command for the organization where the breach occurred. **(T-0).**

3.2.5. Commanders/Directors shall ensure that individuals who are responsible for causing the breach receive refresher training entitled, "Defense Information Systems Agency Identifying and Safeguarding Personally Identifiable Information located at **https://public.cyber.mil/**. Commanders may also take any appropriate disciplinary action. **(T-1).**

3.2.6. United States Computer Emergency Response Team Reported PII Incidents. According to Chairman Joint Chiefs of Staff Manual 6510.01B, *Cyber Incident Handling Program*, Enclosure C, "When a Computer Network Defense Service Provider discovers compromised or potentially compromised PII, they must notify the United States Computer Emergency Response Team and their servicing Privacy Office." United States Computer Emergency Response Team is responsible for analyzing and reducing cyber threats, vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities. United States Computer Emergency Response Team shall follow through on Computer Network Defense Service Provider detections of PII Incidents by notifying the Information Security Officer and Program/Project Manager of the web application and/or Information Technology system cited. **(T-0).**

3.2.7. The information security officer and Program/Project Manager of the application or system from which the breach occurred, must notify the servicing privacy manager or monitor. That servicing privacy manager shall make appropriate breach notifications established by AF Policy and DoD reporting guidance. **(T-0).**

Chapter 4

THE PRIVACY ACT OF 1974

4.1. Overview of the Privacy Act of 1974.

4.1.1. Under the Privacy Act of 1974, The Congress finds the following:

4.1.1.1. The privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies is protected under The Constitution of the United States.

4.1.2. Provides certain safeguards for an individual against an invasion of personal privacy. It does this by requiring Federal agencies, except as otherwise provided by law, to:

4.1.2.1. Permit an individual to determine what records pertaining to him/her are collected, maintained, used, or disseminated by such agencies or be made available without his/her consent.

4.1.2.2. Permit an individual to gain access to information pertaining to him/her in Federal agency records, to have a copy made of all or any portion thereof, and to correct or amend such records.

4.1.2.3. Collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current for its intended use, and that adequate safeguards are provided to prevent misuse of such information.

4.1.2.4. Permit exemptions from the requirements with respect to records provided in the Privacy Act only in those cases where there is an important public policy need for such exemption as has been determined by specific statutory authority.

4.2. Privacy Act Responsibilities.

4.2.1. Air Force personnel shall:

4.2.2. Collect, maintain, and use information only for purposes described in the published SORN to support programs authorized by law or executive order and as implemented by DoD and AF prescribing directives. **(T-0).**

4.2.3. Adequately safeguard records. **(T-0). (See chapter 7, Protecting Records).**

4.2.4. Maintain records in accordance with an approved Records Disposition Schedule, which defines the time period records should be maintained and how to properly disposition records, including destruction. **(T-0).**

4.2.5. Ensure records are timely, accurate, relevant, and complete. **(T-0).**

4.2.6. Amend and correct information in a SOR upon request, as appropriate by the owner of the SOR. **(T-0).**

4.2.7. Allow individuals to review and receive copies of record(s) that contain their personal information unless a statutory exemption applies. **(T-0).**

4.2.8. Provide personal information requested through the Privacy Act at the requester's discretion. (e.g., personal e-mail (unencrypted), facsimile, first class mail). **(T-0).**

4.2.9. Use official forms and similar tools that have been approved and published in accordance with AFI 33-360, when collecting PII. **(T-0).**

4.2.10. Ensure individuals are provided a Privacy Act Statement whenever collected information is to be maintained in a System of Records (see **paragraph 4.5**, of this instruction). **(T-0).**

4.2.11. Request an OMB control number whenever information is being collected from ten or more members of the general public, in accordance with the Paperwork Reduction Act, Title 44 United States Code Section 3501. This requirement may apply to Military or Government civilians whenever information is being collected outside the scope of their duty. (See AFI 33-324, *The Air Force Information Collections And Reports Management Program.* **(T-0).**

4.2.12. Air Force personnel (to include contractors) shall not:

4.2.12.1. Maintain a System of Records on individuals without their knowledge and/or without a System of Records Notice published to the Federal Register. Doing so is known as maintaining a "Secret File" on an individual which is a violation of the Privacy Act. Failure by military members or a civilian equivalent to obey the mandatory provision in this paragraph is a violation of Article 92(1) of the UCMJ. **(T-0).**

4.2.12.2. 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 AF has the permission of that individual, the individual posts/sends the record directly to the AF, or is authorized by Federal statute; or the information pertains to and is within the scope of an authorized law enforcement activity. **(T-0).**

4.2.12.3. Penalize or harass an individual for exercising rights guaranteed under the Privacy Act. **(T-0).**

4.2.12.4. Transmit informational materials or communications that contain personal information to or from personal or commercial e-mail accounts unless a written consent has been submitted by the individual who has requested their personal information to be sent to a personal or commercial e-mail account. In addition, the transmission of PHI is restricted, pursuant to guidance in AFMAN41-210 paragraph 6.16. Failure by military members to obey the mandatory provision in this paragraph is a violation of Article 92(1) of the UCMJ. **(T-0).** Civilians who violate information security policy may be disciplined in accordance with AFI 36-704, *Discipline and Adverse Actions of Civilian Employees*.

4.2.12.5. Use auto-forwarding through multiple user accounts to circumvent CAC-based authentication and DoD encryption requirements. **(T-0).**

4.2.12.6. File personal notes in a SOR, as personal notes will be considered part of the SOR. **(T-0).**

4.2.12.7. Use personal information for any other reason not stated under the purpose within the published SORN. **(T-0).**

4.2.12.8. Pull data or information from an approved system of records to be added to an unapproved source for convenience or any other means. (**Note:** Doing so, the data is no longer in the location as prescribed in the SORN published in the federal register.) **(T-0).**

4.3. Privacy Act Complaints and Violations.

4.3.1. A privacy complaint is an allegation that an agency or its employees violated a specific provision of the Privacy Act of 1974, as amended, regarding the maintenance, amendment, or dissemination of personal information in a SOR. A privacy violation occurs when an agency or individual knowingly or willfully fails to comply with provisions of the Privacy Act.

4.3.2. Privacy Act complaints and violations must be submitted in written form to the servicing privacy manager. **(T-0).**

4.3.3. Alleged Privacy Act complaints or violations are processed through the supporting Privacy Manager. The Privacy Manager directs the process and provides guidance to the SOR owner. Issues that cannot be resolved at the local level shall be elevated to MAJCOM Privacy Manager, as appropriate. **(T-1).**

4.3.4. Penalties for Violation. An individual may file a civil law suit against the AF for failing to comply with the Privacy Act. An AF employee may be subject misdemeanor criminal charges and a fine of up to $5,000 may be imposed if he/she:

4.3.4.1. Maintains a SOR without publishing the required SORN in the Federal Register or;

4.3.4.2. Willfully discloses personal information from a SOR, knowing that dissemination is prohibited, to anyone not entitled to receive the information.

4.3.5. Privacy Act and Complaints Reporting Process.

4.3.5.1. The local Privacy Manager or SOR owner shall:

4.3.5.1.1. Conduct an inquiry to determine if a formal investigation of the complaint or allegation of a Privacy Act violation is warranted. **(T-0).**

4.3.5.1.2. Ensure a response is sent to the complainant through the Privacy Official. (**Note:** For Privacy Act complaints filed in a U.S. District Court against the AF, an AF activity, or an AF employee, AFLOA/JAC shall provide SAF/CNZA 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, the Office of The Judge Advocate's General Litigation Division will send SAF/CNZA a copy of the judgment and opinion. **(T-1).**

4.4. Maintaining Privacy Act Information. Each organization that maintains a SOR shall:

4.4.1. Maintain in its records only information about an individual that is relevant and necessary to accomplish a purpose of the agency as required by a statute or executive order or their implementing regulations. **(T-0).**

4.4.2. To the greatest extent practicable, collect personal information only directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs.

4.4.2.1. Examples of when it is more practical to collect information from a third party instead of the subject individual include but are not limited to, the following:

4.4.2.1.1. Verification of information through third-party sources for security or employment suitability determinations. **(T-0).**

4.4.2.1.2. Seeking third-party opinions such as supervisor comments as to job knowledge, duty performance, or other opinion-type evaluations. **(T-0).**

4.4.2.1.3. Obtaining information first from the individual may impede rather than advance an investigative inquiry into the actions of the individual. **(T-0).**

4.4.2.1.4. 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. **(T-0).**

4.4.2.1.5. Implementing and enforcing safeguards to ensure protection of personal information. **(T-0).**

4.4.2.1.6. Collection of personal information for the purpose of pilot program is prohibited unless a System of Records Notice is published in the Federal Register prior to the collection. **(T-0).**

4.4.3. Ensuring required Privacy Act Statement is provided to individuals when personal information is collected. **(T-0).**

4.4.4. In accordance with 44 USC § 3501, an OMB control number shall be requested whenever information is being collected from ten or more members of the general public. This requirement may apply to Military or Government civilians whenever information is being collected outside their scope of their duty. (See AFI 33-324) **(T-0).**

4.5. Privacy Act Statements.

4.5.1. Whenever an individual is requested to provide personal information that will be maintained in a SOR or collected on an official AF Form, the individual shall be provided the authority, purpose, routine use(s), whether disclosure of the information is voluntary or not; and the applicable SORN. This is known as a Privacy Act Statement.

4.5.1.1. Authority: the legal authority that authorizes the solicitation of the personal information. **(T-0).**

4.5.1.2. Purpose: the principal purpose or purposes for which the information is intended to be used. **(T-0).**

4.5.1.3. Routine Uses: who will the personal information be shared with on a routine basis outside the DoD. **(T-0).**

4.5.1.4. Disclosure: Voluntary or Mandatory. (Use mandatory only when disclosure is required by law and the individual will be penalized for not providing information. All mandatory disclosure requirements must first be reviewed by the servicing legal office). Include any consequences of nondisclosure in nonthreatening language. **(T-0).**

4.5.1.5. AF SORN(s), are searchable by number and title, and are available at: **https://dpcld.defense.gov/privacy/SORNS.aspx** (If applicable) **(T-0).**

4.5.2. Privacy Act Advisory Statements in Publications. Include a Privacy Act Advisory Statement in each AF publication that requires collecting or keeping personal information in a SOR. Also include a statement when publications direct collection from the individual of any part or form of the Social Security Number (SSN). The statement shall refer to the legal authority for collecting the information and SORN number and title as follows: **This**

instruction 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, and regulation]. The applicable System of Records Notice(s) [number and title] is (are) available at: https://dpcld.defense.gov/privacy/SORNS.aspx (T-0).

4.5.3. Label: Air Force Visual Aid (AFVA) 33-276, *Air Force Privacy Act Label*. Use is mandatory to assist in identifying Privacy Act information by placing the label on the covers of removable electronic storage media such as laptops, Government hard drives, DVDs, CDs, diskettes, tapes and may be used for deployment folders. The label is not authorized for use on file drawers, file cabinets, mailing envelopes, or other stationary equipment or materials in accordance with AFI 33-322, *Records Management and Information Governance Program*. **(T-1).**

4.5.4. The Privacy Act requires agencies to provide safeguards to ensure the security and confidentiality of SOR and to protect individuals against an invasion of personal privacy.

4.6. Publishing System of Records Notices (SORNs). The AF Privacy Officer will submit SORNs to the Defense Privacy and Civil Liberties Transparency Division (DPLTD) to be published in the Federal Register for new, changed or deleted SOR. When published, the public will be allowed 30 days to comment. Collection of this information is not authorized until the SORN is final, including during this 30 day review period. If comments are received that result in a contrary determination, this could further delay the time until a final SORN is published and collection may occur. Any collection conducted prior to finalizing the SORN is an illegal collection and can result in civil penalties under the Privacy Act of 1974 5 USC § 552a as amended, (i)(1) Criminal Penalties. **(T-0).**

4.6.1. When is a SORN required? A SORN is required when personal information is maintained on an individual and is regularly retrieved by a name, number (DoD ID number, Social Security number, etc.), symbol, or other identifying particular (data element) assigned to the individual. The Privacy Act requires submission of new or significantly changed SORNs to the OMB and both houses of Congress before publication in the Federal Register. There are 3 types of SORN Action requests (new, modification, and rescindment) that can be submitted. Refer to DoD SORN Reference Guide located at AF Privacy SharePoint® site:

https://cs2.eis.af.mil/sites/10440/InfoAcc/Privacy/Risk%20Management%20Framework%20(RMF)%20Privacy%20Process/3.%20SORN%20REFERENCE%20GUIDE,%20Version%20II,%20May%202018.pdf

4.6.2. Other Systems. National Security SORs require a 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).

4.6.3. Adopting Existing SORN. A new or existing SOR may be incorporated into an existing SORN published in the Federal Register:

4.6.3.1. First, research current SORNs, including those that cover systems of records government-wide and DoD-wide on the Defense Privacy Notices website at **https://dpcld.defense.gov/privacy/SORNS.aspx** for one that matches well with the new SOR at all points, i.e., Category of Individuals Covered, Category of Records, Authority, Purposes, Routine Uses, Policies, etc.

4.6.3.2. 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 AF SOR and POC information.

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

4.6.5. Updating SORNs. Examples for Adding, Altering, Amending, and Deleting a SORN are available on the AF Information Access SharePoint® and the AF Privacy Website.

4.6.6. Submitting SORNs for publication in the Federal Register. The Program/Project Manager must submit the proposed SORN through their MAJCOM Privacy Manager at a minimum of 120 days before the planned implementation date of a new SOR or a change to an existing SOR subject to this instruction. The Privacy Manager shall review for accuracy and completeness and send electronically to the AF Privacy Office **usaf.pentagon.saf-cn.mbx.af-privacy@mail.mil**. The AF Privacy Office shall review and forward to Defense Privacy, Civil Liberties, and Transparency Division for review and publishing in the Federal Register, as appropriate. **(T-1).**

4.6.7. Requirement for continuous monitoring review of published SORNs. Program/Project Managers shall ensure that no system of records includes information about an individual that is not relevant and necessary to accomplish a purpose required by statute or executive order (Appendix I to OMB Circular A-108), (Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act). PMs review and submit any changes through the process described in this chapter and promptly update appropriate answers to Information Technology Investment Portfolio Suite questions. **(T-0).**

4.6.8. Rescindment of SORNs. If an IT system is being decommissioned or closed and has a published SORN that is no longer required, comply with DoD SORN Reference Guide and OMB A-108, Appendix IV Office of the Federal Register SORN template - Notice of Rescindment and submit appropriate deletion request to the AF Privacy Office, **usaf.pentagon.saf-cn.mbx.af-privacy@mail.mil** to be forward to DoD to have the SORN deleted from the Federal Register. **(T-1).**

4.7. Privacy Act Records Request. Persons or their designated representatives may ask for a copy of their records maintained in a SOR. Requesters need not state why they want access to their records. Personnel who receive requests must verify the identity of the requester to avoid unauthorized disclosures. How their identity is verified 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 a request via telephone as appropriate or e-mail, a notarized statement, or an unsworn statement. An unsworn declaration or notarized statement should be obtained in the following format:

4.7.1. Requesting Access to Records in a SOR.

4.7.1.1. Contents of Request. “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).”

4.7.1.1.1. Description of Records. The requester must adequately describe the records they want. The requester is not required to name a SOR, but they should at least name

a type of record or functional area. For requests that ask for "all records about me," the requester should be asked for more information about the types of records they are seeking and informed as to how their input can help the AF respond as quickly as possible. If the requester needs help identifying types of systems or records, provide them information to review the government-wide systems of records published in the Federal Register and AF specific SORNs published at **https://dpcld.defense.gov/privacy/SORNS.aspx**. Ensure they understand that identifying the relevant SORN(s) will make the AF review more efficient. If the requester is truly requesting all records pertaining to themselves or an individual, inform the requester they must make a Freedom of Information Act (FOIA) request. **(T-0).**

4.7.1.1.2. Provide Verification of Identity. **(T-0).**

4.7.1.2. Use of a Government Resource to make a request is prohibited. **(T-0).**

4.7.2. Processing a Request for Access to Records in a SOR. Immediately consult the local Privacy Manager, if necessary, to ensure timely response to the request. When individuals request information about themselves, they are not required to cite either the Privacy Act or Freedom of Information Act (FOIA). The individual who processes the request will apply the Privacy Act when records are contained in a SOR and will apply the FOIA to all other records. **(T-0).**4.7.2.1. Acknowledge Request. As a good practice SOR owner should send the requester an acknowledgement letter within 10 workdays informing them of an approximate completion date. **(T-0).**

4.7.2.1. Required Response. As a good practice SOR owner should provide a copy of the record(s) to the requester within 20 workdays of receiving the request. If the SOR has an exemption, inform the requestor of those exemptions in a format the requester can understand. If the system is exempt from disclosure under the Privacy Act, follow the procedures addressed in **paragraph 4.7.3 (T-0).**

4.7.3. Denying or Limiting Access. When information protected under the Privacy Act may 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 DoDM 5400.07_AFMAN 33-302, *Freedom of Information Act Program*, are followed. For Privacy Act denials also processed under the FOIA (**Note:** This should be an extremely rare circumstance), send a copy of the request, the record copy, and why access has been denied (include the applicable exemption) to the denial authority through the legal office and the Privacy Office. The servicing legal office shall include a written legal opinion. The legal opinion shall not merely state that the decision is "legally sufficient," but shall provide factual details and an analysis of the law and applicable regulations. The Privacy Manager 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.

4.7.3.1. Before a request for access to a Privacy Act System of Records from the subject is denied that was not processed under the FOIA, the SOR owner shall ensure that:

4.7.3.1.1. The system has an exemption published in the Federal Register as a final rule. **(T-0).**

4.7.3.1.2. The exemption covers each document. All parts of a system are not automatically exempt. **(T-0).**

4.7.3.1.3. The FOIA does not require release of any part of the record. **(T-0).**

4.7.3.1.4. Nonexempt parts are segregated. **(T-0).**

4.7.4. Third Party Information in a SOR. A first party requester is not entitled to receive information that does not directly pertain to him or her that is contained in their record; for example, the home address or SSN of a third party that is contained in their system of record solely for ease of identification of the 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 SOR. **(T-0).**

4.8. Amending a Privacy Act Record.

4.8.1. Amendment Reasons. Individuals may ask to have their personal information in a SOR amended to make such information accurate, timely, relevant, and complete. System managers shall routinely correct a record if the requester can show that it is factually incorrect (e.g., date of birth is wrong). **(T-0).**

4.8.2. Responding to Amendment Requests.

4.8.2.1. The individual may request simple corrections orally. Requests for complicated and detailed corrections must be in writing to ensure clarity. **(T-0).**

4.8.2.2. After verifying the identity of the requester, the receiving agency shall make the change if appropriate, notify all known recipients of the record, and inform the affected individual. **(T-0).**

4.8.2.3. Acknowledge requests within 10 workdays of receipt. Give an expected completion date unless the change is completed within that time. Final decisions must, unless extended by the appropriate authority, take no longer than 30 workdays after the date of receipt. **(T-0).**

4.9. Approving or Denying a Record to be Amended. The AF 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 the requester may:

4.9.1. If the SOR owner decides not to amend the record then a copy of the request, the record, and the recommended denial reasons shall be sent to their servicing legal and Privacy Office. Legal office shall include a written legal opinion. The legal opinion shall not merely state that the decision is "legally sufficient," but will provide factual details and an analysis of the law and applicable regulations. **(T-0).**

4.9.2. The SOR owner shall send the requester a letter with the decision. **(T-0).**

4.9.3. If the SOR owner denies the request to amend the records, the requester may file a concise statement of disagreement with the Air Force Privacy Officer.

4.10. Contents of Privacy Act Processing Case Files. Copies of disputed records shall not be kept in Privacy Act Processing case files. Disputed records shall be filed under their appropriate series. Use the Privacy Act Processing case files solely for statistics and to process requests. Such case files shall not be used to make any kind of determination about an individual. The reasons for

untimely responses shall be documented in the Privacy Act Processing case files and may include the following:

4.10.1. Requests from and replies to individuals on whether a SOR contains records about them. **(T-0).**

4.10.2. Requests for access or amendment. **(T-0).**

4.10.3. Approvals, denials, appeals, and final review actions. **(T-0).**

4.11. First Party Appeal Process for Denial to Access or Amendment of a Privacy Act Record.

4.11.1. Appeals 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.

4.11.2. The SOR owner shall promptly send a complete appeal package to the Air Force Privacy Officer. The package must include the following:

4.11.2.1. The original appeal letter; **(T-0).**

4.11.2.2. The initial request; **(T-0).**

4.11.2.3. The initial denial; **(T-0).**

4.11.2.4. A copy of the record; **(T-0).**

4.11.2.5. Any internal records or coordination actions relating to the denial and the denial authority's comments on the appellant's arguments and the legal reviews. **(T-0).**

4.11.3. If the SOR owner reverses their decision on an earlier denial and grants access or amendment, notify the requester immediately.

4.11.4. The SOR owner may include a brief summary of the reasons for not amending the record.

4.11.5. The Air Force Privacy Officer will review the denial and provide a final recommendation to the SOR owner along with providing the requester with the final AF decision and explanation of judicial review rights. **(T-0).**

4.11.6. The records will clearly show that a statement of disagreement is filed with the record or separately, if applicable. **(T-0).**

4.11.7. The disputed part of the record must show that the requester filed a statement of disagreement. **(T-0).**

4.11.8. 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.

4.12. Disclosing Information.

4.12.1. In all cases, use the following guidelines to decide whether to release information without consent:

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

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

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

4.12.2. Rules for Releasing personal information without Consent of the Subject. The Privacy Act prohibits disclosure of personal information within a SOR without the prior written consent of the individual to whom the record pertains. There are twelve exceptions to the "no disclosure without consent" rule. (See **https://www.privacy.af.mil/Home/Privacy-Act-Exceptions/**.)

4.12.3. Disclosing the Medical Records of Minors. AF 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 and/or circumstances under which minors are consider emancipated. Consult with the servicing legal office's medical liaison and Military Treatment Facility for guidance to the age of majority, especially in overseas locations.

4.12.4. Disclosure Accountings. System managers must keep an accurate record of all disclosures made from any SOR except disclosures to DoD personnel for a valid 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.

4.12.4.1. System managers shall file the Accounting of Disclosure record and give it to the data 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:

4.12.4.1.1. Release date. **(T-0).**

4.12.4.1.2. Description of information. **(T-0).**

4.12.4.1.3. Reason for release. **(T-0).**

4.12.4.1.4. Name and address of recipient. **(T-0).**

4.12.4.1.5. Some exempt systems let you withhold the accounting record from the subject. **(T-0).**

4.12.4.1.6. Withhold information about disclosure accountings for law enforcement purposes at the law enforcement agency's request. **(T-0).**

4.13. Computer Matching. Computer matching programs electronically compare records from two or more automated systems, one from the DoD and the other from a Federal agency, or a state or local government in order to make a decision that affects an individual's rights, benefits and/or privileges.

4.13.1. A system manager proposing a match that could result in an adverse action against a Federal employee must meet the following requirements of the Privacy Act:

4.13.1.1. Prepare a written agreement between participants; **(T-0).**

4.13.1.2. Secure approval of the Defense Data Integrity Board; **(T-0).**

4.13.1.3. Publish a matching notice in the Federal Register before matching begins; **(T-0).**

4.13.1.4. Ensure full investigation and due process; and **(T-0).**

4.13.1.5. Act on the information, as necessary. **(T-0).**

4.13.2. The Privacy Act applies to matching programs that use records from Federal personnel or payroll systems and Federal benefit programs where matching:

4.13.2.1. Determines Federal benefit eligibility;

4.13.2.2. Checks on compliance with benefit program requirements; or

4.13.2.3. Recovers improper payments or delinquent debts from current or former beneficiaries.

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

4.13.4. Any activity that expects to participate in a matching program must contact the AF Privacy Officer immediately. System managers must prepare a Computer System Matching Agreement notice for publication in the Federal Register, which explains the routine uses that permit the processing of personal information to the AF Privacy Officer. Allow 180 days for processing requests for a new matching program. **(T-0).**

4.13.5. Individuals must receive notice when they are asked to provide personal information that will be used in a matching program as a routine use. The most appropriate method of providing notice is to include the Privacy Act Statement on the form used when an individual applies for benefits. When the individual completes and submits the form and has been provided adequate notice, they are consenting to the routine uses associated with the notice. Coordinate appropriate statements with the MAJCOM Privacy Manager and AF Privacy Officer. **(T-0).**

4.14. Privacy Act Exemptions.

4.14.1. Exemption Types. This section contains the most current exemptions that have been published as final rules for the listed SOR as of the date of this instruction. The Information System Owners should ensure that a more recent final rule has not been published. There are two types of exemptions from release or disclosure permitted by the Privacy Act:

4.14.1.1. A General exemption authorizes the exemption of a SOR from most parts of the Privacy Act.

4.14.1.2. A Specific exemption authorizes the exemption of a SOR from only a few parts of the Privacy Act.

4.14.2. 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 SOR has been published in the Federal Register as a final rule. (See **https://dpcld.defense.gov/privacy/SORNS.aspx**; exemptions are noted in the right column.)

4.14.3. Requesting an Exemption. An ISO who believes that a system requires an exemption from some or all of the requirements of the Privacy Act shall send a request through the Wing

Privacy Office, the MAJCOM Privacy Office, and to AF Privacy Office. Final approval is granted by Defense Privacy, Civil Liberties, and Transparency Division. 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.

4.14.4. Exemptions. Exemptions permissible under the Privacy Act are searchable at **http://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a.pdf** **(T-0)**.

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

4.14.4.2. The (k)(1) exemption. Applies to information specifically authorized to be classified according to DoDM 5200.01.

4.14.4.3. 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 AF 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). **(T-0).**

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

4.14.4.5. 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 United States Code Section 8; Authenticated transcripts or copies of certain returns; other data; restriction on use; disposition of fees received.

4.14.4.6. The (k)(5) exemption. Applies to investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for U.S. civilian employment, military service, U.S. 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.

4.14.4.7. 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.

4.14.4.8. 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 5

E-GOVERNMENT ACT

5.1. Overview of the E-Government Act of 2002, 44 USC § 3601.

5.1.1. The E-Government Act of 2002 establishes business processes to "provide enhanced access to Government information and services in a manner consistent with laws regarding protection of personal privacy, national security, records retention, and access for persons with disabilities, and other relevant laws." The Act inserted the Privacy Impact Assessment (PIA) into the government IT lifecycle. PIAs are required for all IT systems that collect, maintain, or disseminate information in identifiable form or that make substantial changes to existing information technology that manages information in identifiable form. PIA implementation for DoD IT investments is defined in DoDI 5400.16.

5.2. Privacy Impact Assessments (PIA).

5.2.1. Evaluate Information Systems Risk Management Framework. Information System owner (ISO), Information System Security Manager (ISSM), Information System Security Officer (ISSO), Portfolio Managers, and Program Managers/Project Managers shall address risks assessment on PII in an IT system and plan the integration of privacy protections with appropriate Information Assurance (IA) controls into the development life cycle of an information system. A PIA shall be completed in accordance with DoDI 5400.16. **(T-0).**

5.2.2. What is a PIA? A PIA is an analysis of how information in identifiable form is collected, stored, protected, shared, and managed. The purpose of a PIA is to demonstrate that system owners and developers have incorporated privacy protections throughout the entire life cycle of a system.

5.2.3. When must a PIA be conducted?

5.2.3.1. The E-Government Act of 2002 and DoDI 5400.16 require PIAs to be conducted before 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.

5.2.3.2. PIAs are required to be performed, approved 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 to include National Security System and systems that do not contain PII. **(T-1).**

5.2.3.3. If applicable, a SORN containing the most up-to-date and accurate information will accompany the PIA. The PIA should reflect the categories of records, categories of individuals, record source, authorities, purpose, routine uses, notification procedures, safeguards, and retention/disposal as outlined in the SORN.

5.2.3.4. When the PIA is submitted to the Air Force Privacy Officer, it must be accompanied by documentation of the PII Confidentiality Impact Level (PCIL) as identified in National Institute Standards of Technology (NIST) SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*. Note, a PCIL is not needed if a system do not contain PII. Additional resources on determining the PCIL can be found at the AF Privacy SharePoint® site:

https://cs2.eis.af.mil/sites/10440/infoacc/privacy/forms/allitems.aspx?RootFolder=%2Fsites%2F10440%2FInfoAcc%2FPrivacy%2FRisk%20Management%20Framework%20%28RMF%29%20Privacy%20Process&FolderCTID=0x012000026A42C21F9EFE4FAA951182BB56DCE6&View=%7BAC017FFA%2D42FE%2D42A0%2DA2D2%2D699CCCA7E366%7D (T-1).

5.2.4. When a PIA must be submitted. PIAs are submitted 120 days from the scheduled operational or expiration date of the Authorization to Operate or Interim Authorization to Operate on all new and existing systems.

5.2.5. Who conducts the PIA? The ISO shall conduct a PIA in conjunction with the system Program Manager/Project Manager, Information System Security Managers and Privacy Manager/Monitor. **(T-0).**

5.2.6. Medical IT systems that are Defense Health Agency (DHA) funded or in the AF line-funded portfolio and managed by Air Force Medical Service assets, shall route PIAs through the DHA Chief Information Officer (CIO) office for appropriate management, signatures, and oversight. **(T-0).**

5.2.7. All DoD Medical Department IT systems purchased with DHA funds must only be reported to the DoD Information Technology Portfolio Repository via the component Defense Health Agency (DHA). **(T-0).**

5.2.8. Format and Digital Signatures. PIAs shall be completed on DD Form 2930, *Privacy Impact Assessment (PIA)*, as an unsecured fillable PDF which requires digital signatures as follows, except for medical Defense Health Program funded systems.

5.2.8.1. Privacy Impact Assessments processing procedure.

5.2.8.1.1. The system Program/Project Manager will digitally sign and forward the signed PIA to their perspective ISSM/ISSO. **(T-0).**

5.2.8.1.2. Information Systems Security Managers digitally sign and forward the signed PIA to their Base Privacy Manager. Base Privacy Managers digitally sign and coordinate with the applicable records management office to ensure appropriate lifecycle management of any records created are maintained, used, preserved, and disposed of in accordance with DoDI 5015.02 and National Archives and Records Administration approved records schedules. Records managers annotate in section 3, part f, of the DD 2930, "Records maintenance is consistent with National Archives and Records Administration schedule." Records managers return the PIA to the PM. PMs forward the signed PIA for review to their respective MAJCOM Privacy Office. After MAJCOM review, forward the PIA to AF Privacy Officer for review at **usaf.pentagon.saf-cn.mbx.af-privacy@mail.mil**. AF Privacy Officer will forward to the Senior Information Security Officer CISO workflow e-mail at **usaf.pentagon.saf-cn.mbx.cnz-workflow@mail.mil (T-1).**

5.2.8.1.3. The Senior Information Security Officer or designee shall review, digitally sign and return the signed PIA to the AF Privacy Officer Workflow e-mail **usaf.pentagon.saf-cn.mbx.af-privacy@mail.mil**. **(T-1).**

5.2.8.1.4. The AF Privacy Officer shall digitally sign and forward the signed PIA to the Air Force Chief Inforrmation Officer or representative. **(T-1).**

5.2.8.1.5. The Air Force Chief Information Officer or representative shall digitally sign and return PIA to the AF Privacy Officer. **(T-1).**

5.2.9. Submitting Approved PIAs. AF Privacy maintains a copy of all approved PIAs on the AF Privacy public access website **https://www.privacy.af.mil/Home/PIA/**. An electronic copy will be forwarded by the AF Privacy Officer to the Department of Defense, Chief Information Officer (DoD CIO).

5.2.10. Periodic Reviews and Updates Cycle of PIAs. PMs review and update PIAs in accordance with DoDI 5400.16.

Chapter 6

SOCIAL SECURITY NUMBER (SSN) REDUCTION PLAN

6.1. Social Security Number (SSN) Reduction Plan. 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 in accordance with DoDI 1000.30, *Reduction of Social Security Number (SSN) Use Within DoD*. The Functional office that owns the record for which SSNs are required to be collected is the Office of Primary Responsibility (OPR) for submitting a SSN Justification memorandum with respect to the collection of SSNs for those records. Records Professional, Privacy Manager, and Forms Manager will assist to ensure compliance with the SSN reduction plan requirements. As such there is no need to use the SSN for individuals to authenticate themselves as part of every transaction. DoDI 1000.30, is in effect and establishes the following:

6.1.1. 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 DoD, 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 continuing to collect SSNs. **(T-0).**

6.1.2. Documenting Acceptable Uses of SSN and other PII specifically. The authorization for use of PII is governed through DoD 5400.11-R. 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. **(T-0).**

6.1.3. 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 of the SSN justification shall be retained and available upon request. **(T-0).**

6.2. The Specific Requirement for Use of the SSN.

6.2.1. Forms that collect SSN must have a completed AF Form 673 and a justification memorandum stating the justification for use of the SSN that is addressed to and approved by AF Privacy Officer. Submit items to appropriate Forms Manager in accordance with AFI 33-360. **(T-1).**

6.2.2. A senior official (flag officer or SES equivalent) shall sign the SSN Justification Memorandum stating the justification for use of the SSN. It is unacceptable to collect, retain, use or transfer SSN without an approved justification. **(T-1).**

6.2.3. The SSN Justification Memo that approves collection of 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 Office for approval/disapproval. (See **Attachment 5**.) **(T-1).**

6.2.4. The Defense Privacy, Civil Liberties, and Transparency Division reviews SSN justifications for IT systems as an adjunct to the biennial PII review process. When 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. **(T-0).**

6.2.5. 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 memos shall be reviewed in conjunction with the FISMA Annual review. **(T-0).**

6.2.6. Requesting the Social Security Number (SSN). When requesting an individual's SSN always provide a Privacy Act Statement or Privacy Advisory, as applicable. **(T-1).**

6.3. Alternative Means of Identifying Records. When law, executive order, or regulation does not require disclosing the SSN or if the SOR was created after January 1, 1975, a SSN may be requested, but the individual is not required to disclose it**.** If the individual refuses to provide their information, use alternative means of identifying records. Executive Order (E.O.) 9397, *Numbering System for Federal Accounts Relating to Individual Persons*, November 22, 1943, was amended by E.O. 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 and deletes the mandatory requirement to collecting SSNs. E.O. 9397 (SSN), as amended (E.O. 13478) shall be referenced when cited in a Privacy Act Statement, Privacy Advisory, PIA and SORN whenever a 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 DoDI 1000.30, enclosure 2, paragraph 2, *Acceptable Uses*. Contact the OPR's organizational Privacy Office for assistance. **(T-0).**

6.4. Protection of SSN. SSNs are personal and unique to each individual. The SSN in any form, including, but not limited to truncated (last 4 or 5), 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 a person's SSN to another person without an official need-to-know or consent of the individual. Release of SSNs outside of the DoD is not permitted without the person's consent or unless authorized under one of the twelve exceptions to the Privacy Act (See **https://www.privacy.af.mil/Home/Privacy-Act-Exceptions/**.) **(T-0).**

6.5. Reporting Results of Social Security Number Reduction.

6.5.1. New Departmental Forms. The 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 Act section of the annual FISMA Report as required by Title 44 United States Code, Chapter 35, and Subchapter III. The annual report shall contain the following elements:

6.5.1.1. Number of forms reviewed. **(T-1).**

6.5.1.2. Number of forms requesting SSNs. **(T-1).**

6.5.1.3. Number of SSN justifications accepted and rejected. **(T-1).**

6.5.1.4. Examples of forms where SSNs were not allowed. **(T-1).**

6.5.1.5. Examples of SSN masking or truncation. **(T-1).**

6.5.1.6. For new forms issued below the departmental level (MAJCOM/FOA/DRU, Wing, etc), no database shall be required as set forth in **paragraph 2.6.1**. **(T-1).**

6.5.1.7. Existing Departmental Forms. The AF Departmental Forms Management Officer shall report annually on July 1st the results of the AF Forms reviews and submit a report to the AF Privacy Officer. This report shall include the following elements:

6.5.1.7.1. Total number of forms in the database. **(T-1).**

6.5.1.7.2. Number of forms reviewed. **(T-1).**

6.5.1.7.3. Number of forms containing SSNs. **(T-1).**

6.5.1.7.4. Number of forms where justifications were questioned. **(T-1).**

6.5.1.7.5. Number of SSN justifications accepted and rejected. **(T-1).**

6.5.1.7.6. Examples of forms where SSNs were not allowed. **(T-1).**

6.5.1.7.7. Examples of SSN masking or truncation. **(T-1).**

6.5.1.8. For existing forms issued below departmental level (MAJCOM, Wing, etc.), no reports are required at command and or base levels, with the exception of sharing best practices of specific examples where SSNs were eliminated or better masked, or for metrics collection at the AF level. **(T-1).**

Chapter 7

PROTECTING RECORDS

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

7.1.1. Remove personal information which is accessible through the use of SharePoint® or similar web base applications, when no longer needed for daily operations and properly file in accordance with AF RDS. **(T-0).**

7.1.2. Ensure personal information stored on shared drives, folders, and directories are safeguarded (encrypted or password protected) and accessible only to individuals whose official duties provide them a valid need-to-know. **(T-0).**

7.1.3. Department of Defense Safe Access File Exchange (DoD SAFE) **https://safe.apps.mil/** is an approved alternate means to allows users to transfer large files that contain PII inside and outside the DoD network. Files with PII must be encrypted (password protected) prior to sending through DoD SAFE. In addition, DoD Encryption Wizard will be used as alternate means of safeguarding personal information. (See AFI 41-200, *Health Insurance Portability and Accountability Act (HIPAA)*, for protecting HIPAA information). **(T-0).**

7.1.4. Digitally sign and encrypt e-mail messages, or password protect any attachments containing personal identifiable information. **(T-0).**

7.2. Protecting Personal information or PII Maintained in an Electronic System. It is AF policy that personal information or PII collected, maintained, and stored in an electronic system shall be evaluated by the ISO for impact of loss or unauthorized disclosure and protected accordingly. Ensure coordination is accomplished between IT system PM, ISSM/ISSO and Privacy Manager. (In accordance with AFI 17-130, and DoDI 5400.16).

7.2.1. Assigning PII High, Moderate or Low Impact Security Category. All electronic systems of records shall be assigned a High or Moderate PII impact security category according to the definitions established in this instruction. **(T-0).**

7.2.2. Protect PII of High or Moderate impact security category at a Confidentiality Level of Sensitive or higher as established in DoDI 8500.01, 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).

7.2.2.1. 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 the information. **(T-0).**

7.2.2.2. 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. **(T-0).**

7.2.2.3. Mission assurance category establish the requirements for availability and integrity, and security classification, sensitivity, and need-to-know establish confidentiality requirements. **(T-0).**

7.2.2.4. Enclosure 4 of DoDI 8500.01 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. **(T-0).**

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

7.2.2.5.1. Such records shall not be routinely processed or stored on portable computing devices or removable electronic media without written approval of the ISSM/ISSO. (**Note:** ISSM/ISSO approval is not required in order to remove such records contained on a government laptop computer that is removed from the primary workspace in order to telecommute or travel TDY.) **(T-0).**

7.2.2.5.2. Except for compelling operational needs, any portable 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 8500.01 (hereinafter referred to as "protected workplaces"). (**Note:** Removal of government laptop computers from primary purposes for telecommuting and TDYs is considered a compelling operational need.) **(T-0).**

7.2.3. Electronic Storage Media. Any electronic devices which contain personal information and are removed from their protected workplaces, including those approved for routine processing, shall:

7.2.3.1. Use an AFVA 33-276 to assist in identifying information which may be protected under the Privacy Act by placing the label on the covers of removable electronic storage media. (**Note:** Creation of a Privacy Act label is authorized when approved by functional managers). AF Form 3227 or DD Form 2923 shall be used whenever documents containing personal information are removed from the approved storage area. **(T-0).**

7.2.3.2. Require certificate based authentication using a DoD or DoD-approved Public Key Infrastructure certificate on approved hardware token to access devices. **(T-0).**

7.2.3.3. Implement IA Control PESL-1 (screen lock), with a specified period of inactivity not to exceed 30 minutes (15 minutes or less recommended). **(T-0).**

7.2.3.4. PII Data at Rest on Portable Devices. Encrypt all data at rest, i.e., data that is contained on hard drives or other storage media within portable devices as well as all removable media created by or written from the device while outside a protected workplace. If a portable device is incapable of encryption, it cannot be used to store PII. Minimally, the cryptography shall be NIST-certified (i.e., Federal Information Processing Standard (FIPS) 140-2, *Security Requirements For Cryptographic Modules*, **http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf**). (See DoDI 8500.01, *Cybersecurity*, ECCR-1 (Encryption for Confidentiality (Data at Rest)).) **(T-0).**

7.2.3.5. Follow direction for transmitting PII or other sensitive information via e-mail in accordance with **paragraph 7.3.3** of this instruction. (See also DoDI 8500.01). **(T-0).**

7.2.4. 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 IA Control EBRU-1 (Remote Access for User Functions), EBRP-1 (Remote Access for Privileged Functions), and ECCT-1 (Enclave and Computing Environment) as established in DoDI 8500.01, DoD Memorandum, Department of Defense Guidance on Protecting Personally Identifiable Information (PII).

7.2.4.1. Shall employ certificate based authentication using a DoD or DoD-approved Public Key Infrastructure certificate on an approved hardware token. **(T-0).**

7.2.4.2. The remote device gaining access shall conform to IA Control Physical and Environmental (PESL- 1 screen lock), with a specified period of inactivity not to exceed 30 minutes (15 minutes or less recommended). (See DoDI 8500.01). **(T-0).**

7.2.4.3. The remote device gaining access shall conform to IA Control Enclave and Computing Environment (ECRC-1, Resource Control). (See DoDI 8500.01.) **(T-0).**

7.2.4.4. Download and local/remote storage of records containing PII is prohibited unless expressly approved by the ISO. **(T-0).**

7.3. Maintain a paper or electronic System of Records (SOR) only under the authority of an approved SORN published in the Federal Register (T-0).

7.3.1. Paper or electronic documents and/or materials that contain personal information such as a recall rosters, personnel rosters, lists or spreadsheets shall be marked "FOR OFFICIAL USE ONLY" (See DoDM 5200.01, Volume 4, *DoD Information Security Program: Controlled Unclassified Information (CUI))* as follows: "The information herein is FOR OFFICIAL USE ONLY (FOUO) information which must be protected under the Freedom of Information Act (Title 5 United States Code Section 552) and/or the Privacy Act of 1974. Unauthorized disclosure or misuse of this PERSONAL INFORMATION may result in disciplinary action, criminal and/or civil penalties**." (T-0).**

7.3.2. All paper documents and printed materials that contain personal information shall be covered with the AF Form 3227, *Privacy Act Cover Sheet* or DD Form 2923, *Privacy Act Data Cover Sheet* to protect PII from being viewed by unauthorized personnel when downloaded or removed from their System of Records or approved storage location. **(T-0).**

7.3.3. Exercise caution before transmitting personal information via e-mail to ensure the message is adequately safeguarded. Some information may be so sensitive and personal that e-mail may not be the appropriate means of transmitting. (See DoDI 8500.01, *Cybersecurity*).

7.3.4. When transmitting personal information over e-mail, encrypt and add "For Official Use Only" ("FOUO") to the beginning of the subject line and apply the following statement at the beginning of the e-mail: "This e-mail contains FOR OFFICIAL USE ONLY (FOUO) information which must be protected under the Freedom of Information Act (5 USC § 552) and/or the Privacy Act of 1974. Unauthorized disclosure or misuse of this PERSONAL INFORMATION may result in disciplinary action, criminal and/or civil penalties. Further distribution is prohibited without the approval of the author of this message unless the recipient has a need-to-know in the performance of official duties. If you have received this message in error, please notify the sender and delete all copies of this message." (**Note:** Do not indiscriminately apply this statement to all e-mails. Use it only in situations when you are

actually transmitting personal information required to be protected For Official Use Only purposes. (See DoDM 5200.01. 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). **(T-0).**

7.4. Storing of controlled unclassified information. The storing of any controlled unclassified information on SharePoint® and Shared Drives is permissible providing the user adheres with the established Records Disposition Schedule, the Privacy Act (System of Records Notice, SSN Justification Memorandum (if applicable)) and E-Government Act of 2002; user access is restricted to individuals with a need-to-know to conduct daily operations. Further, PII must be stored on Information Technology (IT) infrastructure that has an authority to operate and has a current Privacy Impact Assessment with the appropriate safeguards for the type of data. Exposed or unprotected PII on SharePoint® and Shared Drives constitutes a potential PII breach and must be reported in accordance with **paragraph 3.1** of this instruction. **(T-0).**

7.4.1. Mail or courier sensitive electronic personal information on any removable media (i.e. CDs, DVDs, hard drives, flash drives, or floppy disks) unless the data is encrypted (See AFI 17-130, *Cybersecurity Program Management*) (see **paragraphs 7.2.2.5.2**, **7.2.3.4**, or **7.2.4.4**, of this publication). **(T-0).**

7.4.2. Return failed hard drives to include copiers with internal hard drives, to a vendor for service if the device was ever used to store Personal Information, without ensuring all data has been permanently removed. **(T-0).**

7.4.3. Leave personal information in unsecured vehicles, unattended workspaces, unsecured file drawers, or in checked baggage. **(T-0).**

Chapter 8

CIVIL LIBERTIES

8.1. Amendments.

8.1.1. First Amendment: Freedom of Religion; Freedom of Speech or of the Press; Right to Peaceably Assemble and to Petition the Government for a redress of grievances. **(T-0).**

8.1.2. Fifth Amendment: Prohibition Against Deprivation of Life, Liberties, or Property, without due process of law. **(T-0).**

8.1.3. Fourteenth Amendment: Due Process and equal protection of the laws. **(T-0).**

8.2. Basic Guidelines. DoDI 5400.11, *DoD Privacy and Civil Liberties Programs* requires at least one senior official designated to advise the Secretary of Air Force (SECAF) on Civil Liberties matters and to meet the following statutory requirements:

8.2.1. Assist the SECAF in appropriately considering Civil Liberties concerns when the AF is proposing, developing, or implementing laws, regulations, policies, procedures, or guidelines related to efforts to protect the Nation against terrorism;

8.2.2. Periodically investigate and review AF actions, policies, procedures, guidelines and related laws and their implementation to ensure that the AF is adequately considering Civil Liberties in its actions;

8.2.3. Ensure that the AF has adequate procedures to receive, investigate, respond to, and provide redress for complaints from individuals who allege that the AF has violated their Civil Liberties;

8.3. Civil Liberties Semi-Annual Report.

8.3.1. The AF Civil Liberties Officer will submit a semi-annual report to Defense Privacy, Civil Liberties, and Transparency Division in accordance with DoDI 5400.11. (See **Attachment 8**). Semi-annual reports are on a fiscal year schedule and are due on the 15th of April and October to the DoD Civil Liberties office. **(T-0).**

8.3.2. AF/A1, SAF/IG, and AF/JAA will submit Civil Liberties reports to SAF/CNZA on the 8th of the month following the end of the quarter in order to meet the DoD suspense date. Civil Liberties reports will not report Civil Liberties complaints in the following circumstances: during the UCMJ process (Courts-Martial/Non-Judicial Punishment); administrative discharge process, or situations whereby an Inspector General Reprisal and restriction complaint may be duplicated. **(T-1).**

8.4. Reprisal For Making Complaint: No AF member, employee, or contractor shall take any action constituting a reprisal, or threat of reprisal, in response to a Civil Liberties complaint or a disclosure of information to a Privacy or Civil Liberties Officer; provided, however, that disciplinary action may be taken if the Civil Liberties compliant or disclosure of information was made with the knowledge that such complaint or disclosure was false, or made with a willful disregard for its truth or falsity. **(T-0).**

8.5. Civil Liberties Training Tools.

8.5.1. The AF Civil Liberties web page includes an overview, and will include Civil Liberties training slides and links to other DoD training on Civil Liberties. “Resources” and “Training.” Can be located here: **https://www.privacy.af.mil/About-Us/Training/ (T-0).**

8.5.2. “The Asylum Seekers Overview.” This online training provided by the Department of Homeland Security provides law enforcement personnel with essential information related to asylum seekers. The course serves as a resource to support the Department of Homeland Security commitment to securing America while providing established protections for asylum seekers. **http://www.dhs.gov/xlibrary/assets/training/xus/crcl/asylumseekers/index.htm**.

8.5.3. The Common Muslim American Head Coverings and Common Sikh American Head Coverings Posters. These posters provide direction to DoD personnel on the appropriate ways in which to screen and, if necessary, search Muslim or Sikh individuals wearing various types of religious head coverings.

WILLIAM E. MARION II, SES, USAF
Deputy Chief Information Officer

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Privacy Act (5 USC § 552a)

Freedom of Information Act (5 USC § 552)18 USC § 3056 (Powers, Authorities, and Duties of United States Secret Service)

18 USC § 1029 (Fraud and Related Activity in Connection with Access Devices)

Paper Reduction Act (PRA) (44 USC § 3501)

44 USC, Chapter 35, Subchapter III (Confidential Information Protection and Statistical Efficiency)

44 USC § 3601-3606, *Public Printing and Documents Chapter 36-Management and Promotion of Electronic Government Services*

13 USC § 8 (Authenticated Transcripts or Copies of Certain Returns; Other Data; Restriction on Use; Disposition of Fees Received)

DoDI 5015.02, *DoD Records Management Program* 24 February 2015

DoDD 1344.10, *Political Activities by Members of the Armed Forces*, 19 February 2008

Office of Management and Budget Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, 3 January 2017

Office of Management and Budget Memorandum 10-22, *Online Use of Web Measurement and Customization Technologies*, 25 June 2010

NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* April 2010

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

Code of Federal Regulations Title 5, section 1320, *Controlling Paperwork Burdens on the Public.*

Chairman Joint Chiefs of Staff Manual (CJCSM) 6510.01B, *Cyber Incident Handling Program*, 10 July 2012

OSD, DA&M Memorandum, *Use of Best Judgement for Individual Personally Identifiable Information (PII) Breach Notification Determinations*, 2 August 2012

Executive Order 13478, Amendments to Executive Order 9397 *Relating to Federal Agency Use of Social Security Numbers*, 18 November 2008

Public Law 107-347, Section 208, *E-Government Act of 2002, Federal Information Security Management Act (FISMA*), 17 December 2002

Public Law 110-53, Section 803, *Privacy and Civil Liberties Officers, Implementing Recommendations of the 9/11 Commission Act of 2007*, 3 August 2007

DoD 5400.11-R, *Department of Defense Privacy Program*, 14 May 2007

DoDI 4500.36, *Acquisition, Management, and Use of Non-Tactical Vehicles (NTVs)*, 11 December 2012

DoDI 6025.18, *Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule Compliance In DoD Health Care Programs*, 13 March 2019

DoDI 8580.02, *Security of Individually Identifiable Health Information in DoD Health Care Programs*, 12 August 2015

DoDI 1000.30, *Reduction of Social Security Number (SSN) Use Within DoD*, 1 August 2012

DoDI 5400.16, *DoD Privacy Impact Assessment (PIA) Guidance*, 14 July 2015

DoDI 8500.01, *Cybersecurity*, 14 March 2014

DoDM 5200.01, Volume 4, *DoD Information Security Program: Controlled Unclassified Information (CUI)*, 24 February 2012

DoDM 5400.07_AFMAN 33-302, *Freedom of Information Act Program*, 27 April 2018

DoDI 5400.11, *DoD Privacy and Civil Liberties Program*, 29 January 2019

Air Force Policy Directive 33-3, *Information Management*, 8 September 2011

Air Force Policy Directive 24-3, *Management, Operations and Use of Transportation Vehicle*, 14 December 2017

AFI 17-130, *Cybersecurity Program Management*, 13 February 2020

AFI 36-704, *Discipline and Adverse Actions of Civilian Employees*, 3 July 2018

AFI 41-200, *Health Insurance Portability and Accountability Act (HIPPA)*, 25 July 2017

AFI 33-322, *Records Management and Information Governance Program*, 6 March 2020

AFI 33-324, *The Air Force Information Collections and Reports Management Program*, 22 July 2019

AFI 33-360, *Publications and Forms Management*, 1 December 2015

AFI 41-210, *TRICARE Operations and Patient Administration Functions*, 10 September 2019

AFI 90-301, *Inspector General Complaints Resolution*, 28 December 2018

AFI 31-218 *Motor Vehicle Traffic Supervision*, 22 May 2006

AFI 24-301, Ground Transportation, 22 October 2019

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

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

Federal Acquisition Regulation (FAR), current edition

Prescribed Forms

AF Form 3227, *Privacy Act Cover Sheet*

AF Form 771, *Accounting of Disclosures*

Adopted Forms

DD Form 2923, *Privacy Act Data Cover Sheet*

DD Form 2930, *Privacy Impact Assessment (PIA)*

DD Form 2959, *Breach of Personally Identifiable Information (PII) Report*

DD Form 2984, *Component Privacy and Civil Liberties Report*

AF Form 847, *Recommendation for Change of Publication*

AF Form 673, *Air Force Publication/Form Action Request*

Abbreviations and Acronyms

AFI—Air Force Instruction

AFIMSC—Air Force Installation Mission Support Center

AFMAN—Air Force Manual

AFPD—Air Force Policy Directive

AFVA—Air Force Visual Aid

CIO—Chief Information Officer

SCOP—Senior Component Official for privacy

CUI—Controlled Unclassified Information

DoD—Department of Defense

DRU—Direct Reporting Unit

FISMA—Federal Information Security Management Act

FOA—Field Operating Agency

FOIA—Freedom of Information Act

FOUO—For Official Use Only

HAF—Headquarters Air Force

IA—Information Assurance

IT—Information Technology

MAJCOM—Major Command

NIST—National Institute of Standards and Technology

OMB—Office of Management and Budget

OPR—Office of Primary Responsibility

PIA—Privacy Impact Assessment

PII—Personally Identifiable Information

SAF—Secretary of the Air Force

SAFE—Department of Defense Safe Access File Exchange / Safe Access File Exchange

SOR—System of Records

SORN—System of Records Notice

SSN—Social Security Number

US—United States

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 SOR 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 SOR 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. 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.

Biometric—Physiological and/or behavioral characteristics that are measurable and can be used to verify the identity of an individual.

Civil Liberties—Fundamental rights and freedoms protected by The Constitution of the United States.

Computer Matching—A computerized comparison of two or more automated systems of records or a SOR 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.

Data Subject—An individual about whom personal information is indexed or may be located under his/her names, personal number, or other identifiable data, in an information system.

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

Federal Agency—A department, independent agency, commission, or establishment of the Executive Branch.

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 SOR. 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.

Incident—An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use polices.

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

Maintain—Includes maintain, collect, use or disseminate in this publication.

Major Command (MAJCOM)—Used throughout this instruction includes MAJCOMs, FOAs, DRUs, and the AFIMSC.

Member of the Public—An individual or party acting in their private life capacity which may include Federal employees or military personnel.

Minor—Under the established age of 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.

Need—to-Know—The authorized, official need based on assigned duties and responsibilities, to access information that is protected under the Privacy Act. There are three cases when a need-to-know may be established: Official business; Statutory; and Information sharing.

PII—Personally Identifiable Information; see Personal Identifier and Personal Information. (e.g., 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.

PII Breach—The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose.**Personal Identifier**—A name, number, or symbol that is unique to an individual and that can be used to trace an individual's 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 or office phone numbers; other demographic, biometric, or personnel information. All information that describes, locates or indexes anything about an individual including his/her education, financial transaction, medical history, criminal or employment record, or that affords a basis for inferring personal characteristics, such as biometric data including finger and voice prints, photographs, or things done by or to such individual; and the record of his/her presence, registration, or membership in an organization or activity, or admission to an institution. Such information is also known as Personally Identifiable Information (PII).

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

Privacy Act Statement—A statement required when soliciting personally identifiable information that is maintained in a SOR (known as Personal Information). The Privacy Act Statement informs the individual why the information is being solicited and how it will be used.

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

Privacy Act System of Records—See SOR.

Privacy Act Complaint—An allegation that the Agency did not comply with specific provisions of the Privacy Act, with respect to the maintenance, amendment, or dissemination of SOR.

Privacy Act Violations—a. When an individual or agency who knowingly and/or willfully 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 willfully maintains a SOR 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. An agency has failed to notify an individual of a system of record(s) being maintained on them; allow an individual access to their record (unless an exemption applies); failure to have a system of record notice published to the federal register; unauthorized access; and obtain access to records under false pretenses.

Privacy Advisory—A statement required when soliciting individual's Social Security Number for the authentication purpose only and will not be maintained in a System of Record. 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 SOR is being created under the Privacy Act.

Program/Project Manager—The individual specifically designated to be responsible for the life cycle management of a system or end item. The Program/Project Manager is vested with full authority, responsibility, and resources to execute and support an approved AF program. The Program/Project Manager is accountable for credible cost, schedule, and performance reporting to the Milestone Decision Authority (DoD 5000.01). Throughout this document the term "Program/Project Manager" is used for consistency with DoD policy and documentation.

Public or Person—(As defined in 5 Code of Federal Regulations 1320, *Controlling Paperwork Burdens on the Public)* members of the public, or the term "person," include individuals, partnerships, associations, corporations (including government-owned contractor-operated facilities), business trusts, legal representatives, organized group of individuals, state, territory, or local government.

Record—Any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his/her education, financial transactions, medical history, and criminal or employment history and that contains his/her name, or the identifying number, symbol or other identifying particular assigned to the individual, such as a finger or voice print or a photograph

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

System Manager—The official who is responsible for managing a SOR including direction and procedures to operate and safeguard it. 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 (SOR)—A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

System of Records Owner—An individual who maintains a record protected under the Privacy Act.

System of Records Notice (SORN) /or/ Privacy Act System Notice—Refers to a legal document that describes the kinds of personal data collected and maintained in a SOR, on whom it is maintained, what the records are used for, and how an individual may access or contest the records in the system. The official public notice published in the Federal Register of the existence, content, and Points of Contact for the SOR containing Privacy Act data. (**Note:** A SORN must be published in the Federal Register to allow the general public a 30-day opportunity to comment before implementing a SOR.)

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

EXAMPLES OF PRIVACY ACT STATEMENT AND ADVISORY STATEMENT

A2.1. Sample Privacy Act Statement. Authority: Title 10 United States Code Section 9013, Secretary of the Air Force; DoDI 4500.36, *Acquisition, Management, and Use of Non-Tactical Vehicles (NTVs)*; Air Force Policy Directive 24-3, *Management, Operations and Use of Transportation Vehicles*; AFI 24-301, *Transportation and Vehicle Operations*; E.O. 9397 (SSN), as amended.

Information is collected to verify your eligibility to drive government owned or leased vehicles exceeding 10,000 pounds; emergency response equipped with four-wheel-drive.
Routine Use: Information may be disclosed for any of the Standard Routine Uses.
Disclosures: Voluntary; however, failure to provide the information may result in our inability to provide you with a government vehicle operator identification card.
System of Records Notice: F024 AF IL C Motor Vehicle Operator's Records.

A2.2. Sample Privacy Advisory. Authority: The Federal Records Act, Title 18 United States Code Section 1029, Access Devices; E.O. 9397 (SSN), as amended.

Disclosure of your SSN is voluntary; however, if you fail to provide your SSN, we will be unable to grant you access to the XYZ database.
Uses to be made of your SSN: Your SSN will be compared against the master list of employees for the sole purpose of positively identifying you. It will not be shared with anyone outside DoD. Once we have confirmed your identity, we will destroy this form.
This data collection will not become part of any Privacy Act System of Record.

Attachment 3

RISK ASSESSMENT

A3.1. Risk Notification. 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, embarrassment, inconvenience or unfairness surrounding the breach. The factors used in assessing the likely risk of harm are:

A3.1.1. Nature of Data Elements Breached. Consider context of the data involved and the potential harm, embarrassment, inconvenience or unfairness that might be generated by its exposure to unauthorized individuals.

A3.1.2. 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. The greater the risk that the information may be used unlawfully should influence an agency's decision to provide notification to the individual(s).

A3.1.3. Likelihood the breach may lead to harm, embarrassment, inconvenience or unfairness to an individual.

A3.1.3.1. Broad Reach of Potential Harm, Embarrassment, Inconvenience or Unfairness. Consider the possible harm associated with the loss or compromise of the PII, i.e., loss of self- esteem, mental pain or emotional stress.

A3.1.3.2. Likelihood Harm, Embarrassment, Inconvenience or Unfairness Will Occur. Agencies must determine the type of data has been compromised and the manner the breach occurred.

A3.1.4. Ability of the Agencies to Mitigate the Risk of Harm, Embarrassment, Inconvenience or Unfairness. In addition to containing the breach, agencies must determine what countermeasures will be used to prevent further compromise of the system's PII.

Attachment 4

EXAMPLE PRIVACY BREACH NOTIFICATION LETTER OFFICIAL LETTERHEAD

Dear Mr. John Miller:

On 3 January 2020, an individual assigned to XXX unit, sent an e-mail with an attachment (alpha roster, recall roster, and information document) containing your Personal Information which may be protected under the Privacy Act of 1974 from their government e-mail to their personal e-mail account. i.e. Yahoo, Gmail, or Hotmail. The e-mail contained your name, social security number, residential address, date of birth, personal e-mail address, and home telephone numbers.

Based on the preliminary investigation, we have determined there was no malicious intent.

We recommend you visit the Federal Trade Commission (FTC) on its website at **http://www.consumer.ftc.gov/articles/0275-place-fraud-alert**. The FTC urges that you 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 Air Force does not endorse this site or provide fraud credit protection.

As the commander of xxxxxx, I take this loss very seriously and I am reviewing our current policies and practices to determine what must be changed to preclude a similar occurrence in the future. At a minimum, I will be providing additional training to personnel to ensure that they understand the importance of safeguarding individual's Personal Information at all times and must be treated in a manner that preserves and protects the confidentiality of the individual.

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

Should you have any questions, please call.

Sincerely, Signature Block

(Directorate level or higher)

Attachment 5

PREPARING A DOD SSN JUSTIFICATION MEMORANDUM

Insert Date

MEMORANDUM FOR DEFENSE PRIVACY, CIVIL LIBERTIES, AND TRANSPARENCY DIVISION

THROUGH: *(insert Component name, office)*

SUBJECT: Justification for the Use of Social Security Numbers (SSNs) in Form (Number and Name) / System Name, DoD Information Technology Portfolio Repository (DITPR) ID #

1. System / Form
The (*system/form*) is (*provide an explanation of what the form or system is, what it is intended to do, and who will use the form/system for what purpose*).

2. Documentation
As documented in (*reference a SORN, PIA, PRA, or other applicable documentation) (system/form)* is utilized to collect information from (*insert who*) for the purpose of (*insert purpose).* (If the supporting documentation is not attached with the submission package, state where the information may be found.)

3. Authorized Uses
The justification(s) for the use of the SSN in accordance with DoDI 1000.30, enclosure 2 are: (*Provide the number and title of* ***each*** *Acceptable Use applicable to the system/form and explain how* ***each*** *use is applicable to the system/form.*).

Note 1: Listing Acceptable Uses without explaining how they apply to the form/system will result in the Memorandum being returned to the Component with no action being taken.

Note 2: If collecting the SSN more than once, or collecting SSNs from multiple individuals (e.g. spouse, dependents, etc.), a rationale must be provided for **each** instance.

3a. Migration Plan (for Acceptable Use #11 only)
Provide a Plan of Action, including milestones for the migration from/elimination of the SSN.

4. Point of Contact
For questions related to this memorandum contact (*provide an appropriate POC, complete with email and telephone).*

Official's Name (SES/General Officer)
Title

Attachment 6

APPROVED DOD TRAINING WEBSITES

Identifying and Safeguarding Personally Identifiable Information (PII) is available online:

https://public.cyber.mil/

DoD Mobile Devices training is available online:

https://public.cyber.mil/

The new Social Networking and Your Online Identity training is available online:

https://public.cyber.mil/

Phishing Awareness is available online:

https://public.cyber.mil/

Attachment 7

NOTIONAL COMPLAINT VIGNETTES

Disclaimer: Vignettes are provided for the instructional purpose of teaching how to identify Civil Liberties related issues only. They do not reflect official policies or positions of the Department of Defense.

1. Religion.

a. Scenario: During the work day, a military unit attended a religious themed movie at the base theater. Members were given the choice of watching the movie or cleaning the barracks while the unit watched the movie. A week later a member of the unit submitted a complaint. In his complaint, he said he chose to watch the movie because he viewed cleaning the barracks as punishment, but now he feels like his religious freedom was violated. He does not think a punishment, like cleaning the barracks, should be an alternative to watching a religious themed movie.

b. Civil Liberties Issue: First Amendment; Freedom of Religion. A service member should not be punished for participating or not participating in a religious activity. If the service member's belief that he faced a punishment for not attending the movie is accurate, his unit leadership should be counseled about the necessity of allowing for unit member religious freedom without the threat of punishment.

2. Social Media Use & Operational Security.

a. Scenario: A deployed service member posted a photograph on Facebook. The caption indicated that his team had just returned from a patrol, and the date/time stamp on the photo showed exactly when it was taken. The service member's chain of command told him to take down the photograph, to protect operational security. However, the service member stated that he was using his personal Facebook account, during his personal time (not while on duty), and not claiming to represent or speak for the military.

b. Civil Liberties Issue: Freedom of Speech/Expression. While individuals have a right to express themselves through online social media outlets, such expression must not compromise operational security. DTM 09-026, "Responsible and Effective Use of Internet-based Capabilities," **Attachment 2**, section 5, states that "when accessing Internet-based capabilities using Federal Government resources in an authorized personal or unofficial capacity, individuals shall employ sound operations security (OPSEC) measures." Other regulations, like the "Joint Ethics Regulation and the Standards of Ethical Conduct for Employees of the Executive Branch," prohibit the release of non-public information, require appropriate disclaimers of opinions being expressed, and restrict the use of government computers to access and to manage personal sites during official duty time.

3. Service Members' Political Involvement.

a. Scenario: An active-duty service member placed a bumper sticker on his privately owned vehicle. The chain of command told the service member to remove the sticker, but the service member refused, citing his Constitutional right to freedom of speech and freedom of expression.

b. Civil Liberties Issue: Freedom of Speech/Expression/Assembly (to the extent that showcasing one's political affiliation constitutes assembly). In keeping with the traditional concept that

service members on active duty should not engage in partisan political activity, and that service members not on active duty should avoid inferences that their political activities imply or appear to imply official sponsorship, approval, or endorsement, the military may regulate service members' participation in political activities. According to DoDD 1344.10, *Political Activities by Members of the Armed Forces*, Sec 4.1.1.8. "A member of the Armed Forces on active duty may: display a political bumper sticker on the member's private vehicle." In this case, the Directive regulating such participation allows the service member to display the bumper sticker. Unit leadership should be counseled about DoD policies regulating service members' participation in political activities.

4. Search and Seizure.

a. Scenario: A DoD civilian, employed at a CONUS Air Force base, was randomly selected to have his vehicle searched at the gate. The gate guard inspected the engine compartment, exterior and undercarriage of the vehicle, and the interior of the vehicle, including the glove box and consoles. The employee submitted a complaint to the base Civil Liberties Officer, alleging that a search of the glove box and consoles was excessive and unreasonable.

b. Civil Liberties Issue: Right to be Secure against Unreasonable Searches and Seizures. Installation commanders issue regulations for the protection and security of property or places under their command. The search followed established procedures for vehicle searches, per direction provided in AFI 31-218, *Motor Vehicle Traffic Supervision.* In evaluating this type of case, consider whether a command authorizes the search of glove boxes and consoles. For example, the AFI instructs officials conducting searches of vehicles entering a military installation to "look under all seats, under/behind dash, glove box, consoles, visors, ashtrays and any packages and briefcases."

5. Don't Ask, Don't Tell – With Speech/Religion Implications.

a. Scenario: A service member speaks with a friend, informally on base, about the repeal of Don't Ask, Don't Tell. The service member, consistent with her religion, expressed opposition to homosexuality. The service member's senior overheard comments and told her to stop expressing these views on base. The service member filed a Civil Liberties complaint, alleging that her freedom of speech/religion was violated when she was told to stop expressing her religious views on base.

b. Civil Liberties Issue: Freedom of Speech/Religion. Service members may express moral or religious beliefs, so long as service members do NOT make statements detrimental to good order and discipline, and so long as service members obey lawful orders. Whether or not the service member's Civil Liberties were, in fact, violated is dependent upon whether or not her comments fall within the constraints articulated in the direction above.

6. Carrying Privately Owned Weapons on Military Installations.

a. Scenario: Service member living in family housing on a Marine Corps base is required to report to the Provost Marshall that she possesses a firearm and stores it at her home. The service member filed a complaint with the Civil Liberties POC arguing that the Provost Marshall should not be keeping records on how she exercises her right to keep and bear arms.

b. Civil Liberties Issue: Right to Keep and Bear Arms. In reviewing the service member's complaint, consider whether the Provost Marshall’s requirement to report the firearm is authorized by a base order or other regulation.

7. Civilian Employment Complaint.

a. Scenario: A DoD civilian supervisor typically allows overtime for all employees who volunteer. However, a civilian employee in that office submitted a complaint, alleging that he has not been allowed to work overtime because the supervisor saw him at an anti-war protest on a Saturday last year. His complaint letter alleged that because his supervisor will not allow him to work overtime, his Civil Liberties are being violated.

b. Civil Liberties Issue: Right to Due Process. His complaint about not being allowed to work overtime, when other workers are encouraged to work overtime, could be a recognized employee grievance. Direct him to consider the use of his agency's existing employee grievance process.

8. Member of Public, Pentagon Protests, and Suspicious Activity Reporting.

a. Scenario: A member of the public attended a protest at the Pentagon. He followed all rules and procedures governing the protest, including not making threatening statements or displaying threatening behavior, and complied with instructions from Pentagon Police Officers. The individual submitted a complaint alleging that a civilian employee, employed at the Pentagon, asked each of the protestors to identify themselves and subsequently stated that he was going to identify them in a suspicious activity report, due to their participation in the protest.

b. Civil Liberties Issue: Freedom of Speech, Peaceable Assembly. Consider whether the Privacy Act is implicated by the Pentagon employee’s actions. According to the Privacy Act (5 USC § 552a(e)(7)), “no information shall be maintained on how an individual exercises rights protected by the First Amendment to The Constitution of the United States, including the freedoms of speech, assembly, press and religion, except as follows:

i. When specifically authorized by statute.

ii. When expressly authorized by the individual, group of individuals, or association on whom the record is maintained.

iii. When the record is pertinent to and within the scope of an authorized law enforcement activity.

Attachment 8

CIVIL LIBERTIES COMPLAINT REPORT INSTRUCTIONS

Introduction:

Public Law 110-53, Section 803, *Privacy and Civil Liberties Officers, Implementing* requires the Department of Defense to report its Civil Liberties activities to Congress. In order to comply with that requirement, each DoD Component must submit a semi-annual Component Privacy and Civil Liberties Report, DD Form 2984 to the Defense Privacy, Civil Liberties, and Transparency Division. Defense Privacy, Civil Liberties, and Transparency Division will consolidate Component data and submit the Department's reports to Congress.

Component reports must include the following:

(1) The number and nature of Civil Liberties complaints received; and

(2) A summary of the disposition of such complaints.

Semi-Annual reports are due by the 10th day of the month following the closing of each fiscal year quarter to the AF Civil Liberties POC: **usaf.pentagon.saf-cn.mbx.af-privacy@mail.mil**

Component Points of Contact (POCs) Reporting Responsibilities

POCs are responsible for establishing procedures to report Civil Liberties complaints for their entire Component.

To ensure the Department is accurately accounting for and addressing Civil Liberties complaints, Component reporting procedures should capture Civil Liberties complaints that may be received by offices such as the Inspector General (IG), Equal Employment Opportunity, and Labor Management Employee Relations (LMER). Component reporting procedures should also ensure that there is no duplicate reporting within the Component.

Report Direction

Definitions

Civil Liberties Complaint:

For purposes of reporting, a complaint is an allegation of one or more Civil Liberties violations.

Received:

The Component has received the complaint and is evaluating it for a Civil Liberties implication.

Pending:

The complaint has not been fully adjudicated or resolved.

Resolved:

The complaint has been fully adjudicated or resolved.

Provide a summary of complaints on a separate sheet of paper. Include the following information for each complaint:

1. Description of complaint. Please identify the constitutional amendment, law, regulation, or other authority alleged to be violated in the complaint, if possible.

Do not include any personally identifiable information (PII) about the complainant or any other persons involved in complaint (examples of PII include names, addresses, phone numbers, and Social Security Numbers).

2. Findings; and

3. Disposition.

Examples of Potential Complaints Implicating Civil Liberties (not an exhaustive list):

A military service member claims he was punished by his commanding officer for refusing to attend a religious activity; or by not being allowed to attend a religious function in accordance with his religious beliefs.

A civilian employee made disparaging comments about the Department via his personal social networking page and was instructed by his supervisor to remove the posts, or be reprimanded.

Attachment 9

EXAMPLE COMPONENT PRIVACY AND CIVIL LIBERTIES REPORT (DD FORM 2984)

COMPONENT PRIVACY AND CIVIL LIBERTIES REPORT

1ST QTR FY19 – OCTOBER TO MARCH 2019

DEPARTMENT OF THE AIR FORCE TOTAL NUMBER OF COMPLAINTS: 2

Complaint #1:

Description of Complaint: Complainant alleges his new supervisor sent an e-mail to all-hands announcing that the pre-existing practice of allowing employees to take time away from their desks for religious prayer is being discontinued. Possible First Amendment, Freedom of Religion implication.

Findings: The Department of the Air Force has received and evaluated the complaint, and the complaint is being investigated.

Disposition: Pending.

Complaint #2:

Description of Complaint: Complainant alleges he was reprimanded for attending a political rally during his lunch break. Possible First Amendment, Freedom of Association implication.

Findings: The Department of the Army has received and evaluated the complaint, and the complaint is being investigated.

Disposition: Pending