DEPARTMENT OF THE AIR FORCE
WASHINGTON DC

OFFICE OF THE SECRETARY

AFI 33-332_DAFGM2026-01
25 JUNE 2026

MEMORANDUM FOR ALMAJCOM-ALFLDCOM-FOA-DRU
DISTRIBUTION C

FROM: SAF/CN
1800 Air Force Pentagon
Washington, DC 20330-1800

SUBJECT: Department of the Air Force (DAF) Guidance Memorandum (GM) to Air Force Instruction (AFI) 33-332, Air Force Privacy and Civil Liberties Program

By order of the Secretary of the Air Force, this DAFGM implements changes to AFI 33-332, Air Force Privacy and Civil Liberties Program, dated 10 March 2020. It updates specific roles, responsibilities, and breach-reporting requirements, including revised protocols for handling incidents involving electronic Personally Identifiable Information (PII). This memorandum also directs that any references to Major Commands (MAJCOMs) in AFI 33-332 apply equally to the Secretariat, Air Staff, Space Staff, Field Commands, FOAs, DRUs, and the ANG. In addition, it strengthens civil liberties protections by expanding applicability across all Department of the Air Force personnel categories and removing legacy MAJCOM-only constructs.

Effective immediately, any individual who discovers a potential or actual breach must report it to the servicing Privacy Manager/Monitor without delay. Potential or actual breach will only be entered into the Defense Privacy Information Management System (DPIMS) by the servicing Privacy Manager/ Monitor. The Air Force Installation and Mission Support Center (AFIMSC) must provide immediate notice to the servicing Base Privacy Manager for any breaches reported from Air Forces Cyber, 688th Cyberspace Wing. The servicing Privacy Manager must submit a preliminary PII Breach Report in DPIMS within the prescribed timeline. Breaches must be documented, assessed, and reported in accordance with updated Department of Defense (referred to as the Department of War (DoW)) and DAF guidance. Should any direction in this memorandum conflict with existing DAF publications, the guidance provided herein takes precedence, consistent with DAFI 90-160, Publications and Forms Management.

This memorandum becomes void one year from the date of issuance, or upon publication of an interim change or rewrite of the affected instruction, whichever occurs first. The point of contact for this DAFGM is SAF/CNZA, Compliance Division.

KEITH L. HARDIMAN, SES, DAF
Deputy Chief Information Officer

Attachment:
Guidance Changes to AFI 33-332

ATTACHMENT
Guidance Changes to AFI 33-332

(MODIFY) Purpose: This instruction implements Department of the Air Force Policy Directive (DAFPD) 33-3, Information Management. This instruction applies to all Department of the Air Force personnel, including Regular Air Force, United States Air Force (USSF or Space Force), Air Force Reserve (AFR), Air National Guard (ANG), civilian employees, contractors performing duties under a Department of the Air Force (DAF) contract, and the Civil Air Patrol (CAP) when performing functions for the Department of the Air Force. Use of the term "Major Command" (MAJCOM) throughout this DAFI includes Secretariat, Air Staff, Space Staff, MAJCOMs, Field Commands (FLDCOM), Field Operating Agencies (FOAs), Direct Reporting Units (DRUs), and the Air National Guard (ANG). Failure by military members to comply with the mandatory provisions in paragraphs 3.1.2 and 4.2.12.4 constitutes 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. Civilian employees who violate information security policy may be disciplined in accordance with DAFI 36-148, Discipline and Adverse Actions of Civilian Employees, or DAFI 34-301, Nonappropriated Funds Personnel Management and Administration, as appropriate.

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

(MODIFY) 2.5.1.3. Collect and review Civil Liberties annual Reports for legal sufficiency and provide it to DAF Privacy and Civil Liberties Officer to submit to the Defense Privacy, Civil Liberties, and Transparency Directorate. **(T-1)**

(MODIFY) 2.8. MAJCOM, FLDCOM and Wing or Delta Commanders must:

(MODIFY) 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 or Delta Commander will appoint an installation Privacy Manager/Monitor and Civil Liberties POC and report to their respective command. **(T-1)**

(MODIFY) 2.8.2. Establish policies to notify MAJCOM/Wing or Delta Commander of Privacy Act Violations, complaints and breaches. **(T-1)**

(ADD) 2.8.6.3. Direct an inquiry to determine the circumstances and impact of privacy breaches in accordance with Chapter 3 of this instruction. **(T-0)**

(MODIFY) 2.8.7.1. The DAF Privacy Act web page includes a Privacy Act Overview, Privacy Awareness Video, Privacy Act Exceptions, Resources, DAF System of Record Notice (SORNs), and Privacy Impact Assessment. Go to https://www.privacy.af.mil/.

(MODIFY) 2.8.7.3. Training slides for use by Privacy and Civil Liberties Managers are available on SAF/CNZA SharePoint page.

(MODIFY) 2.8.7.4. Center for Development of Security Excellence Defense Counterintelligence and Security Agency web-based training "DoW Personally Identifiable Information," https://www.cyber.mil/training.

(ADD) 2.8.7.5. Air Education Training Command will work with SAF/CN to author training and publish

with the Enterprise IT & Cyber Infrastructure Division (HNI) to create training in compliance with FISMA, Privacy Act, and other regulations. Users will take training in accordance with same regulations and latest Department of War (DoW) guidance on training.

(ADD) 2.8.7.6. Air Force Life Cycle Management (AFLCMC) DAF365 PMO will deploy material solutions that will enable SharePoint and Teams site owners to enforce compliance. This initiative supports Zero Trust principles by ensuring only properly governed content is discoverable across the organization.

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

(MODIFY) 2.9. MAJCOM, FLDCOM and Base Privacy Managers/Monitors must:

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

(MODIFY) 2.9.5. Report privacy breaches in the Defense Privacy Information System (DPIMS) Breach Reporting System and provide directions to organizations where the breach occurred in accordance with Chapter 3 Breach Procedures. **(T-1)**

(MODIFY) 2.9.10. Submit annual privacy reports and/or other required reports as directed by the DAF Privacy Officer. Annual privacy reports may consist of the number of SORNs reviewed, privacy complaints, and training provided; complaints will be categorized as follows:

(MODIFY) 2.9.12. Base Privacy Managers provide directions to ISO, ISSM/ISSO, and Program Manager/Project Manager for properly completing a SORN and Privacy Impact Assessment (PIA). **(T-1)**

(MODIFY) 2.10. MAJCOM, FLDCOM and Base Legal Offices must:

(MODIFY) 2.11. MAJCOM, FLDCOM and Base Civil Liberties POCs must:

(ADD) 2.15. Department of the Air Force Personnel Center (AFPC).

(ADD) 2.15.1. The Department of the Air Force Personnel Center Directorate of Personnel Support, Military Records Branch (DPS) processes requests for military personnel records submitted on Standard Form 180 (SF-180). As described in DAFI 36-2608, Military Personnel Records Systems, Table A3.2, the Department of the Air Force Personnel Center fulfills record requests for current and former active-duty members of the Department of the Air Force and Space Force components as the Custodian for the Department of the Air Force military records.

(ADD) 2.15.2. Follow the Department of the Air Force Personnel Center Standard Operating Procedure (SOP) which outlines the process for reviewing and responding to non-governmental third-party requests for Department of the Air Force service member records received on the SF-180. Follow established Standard Operating Procedure that requires process and redaction checklists, multiple quality control reviews, and a legal sufficiency review. For third-party non-governmental records requests, Department of the Air Force Personnel Center Judge Advocate (JA) office must review the case file.

(ADD) 2.15.3. For all non-governmental third-party record requests, the service members must authorize release of their record via a signature. Specifically, Section III, Block 5 on the SF-180 – 'Authorized Signature,' must be signed. If the member does not authorize the release via signature on SF-180, the

Military Records Branch is not authorized to release.

(ADD) 2.15.4. A second level review of all third-party requests received by AFPC, elevated to the Chief, Operation Support & Records Management Divisions (GS-14).

(ADD) 2.15.5. The records management team verifies signature of the member in Section III; Block 5 of the SF-180 matches the signature on the source document found in the corresponding member's record in the Automated Records Management System (ARMS).

(ADD) 2.15.6. Follow reinforced procedural safeguards with higher level reviews at the GS-14.

(ADD) 2.15.7. AFPC must establish a quarterly training schedule for PII training.

(ADD) 2.15.8. AFPC must conduct remedial awareness and specialized training to staff members involved in the release process of records requests.

(ADD) 2.15.9. AFPC must conduct a 100 percent quality review of redacted records before release and conduct a monthly audit of all Third-Party requests.

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

(MODIFY) 3.1.3 Air Force Installation and Mission Support Center (AFIMSC) must provide immediate notice to the servicing Base Privacy Manager for any breaches reported from Air Forces Cyber, 688th Cyberspace Wing.

(MODIFY) 3.1.4. The servicing Privacy Manager/Monitor must submit a Preliminary PII Breach Report in the DoW Defense Privacy Information Management System (DPIMS) according to the timeline below. **(T-1)**

(MODIFY) 3.1.5. PII Breach Reports must be completed using the DoW Defense Privacy Information Management System (DPIMS) provided by Defense Privacy and Civil Liberties Directorate only by the servicing Privacy Manager/Monitor. **(T-0)**

(MODIFY) 3.1.6.1. Breach reports MUST not include names of individuals involved or affected by the breach. Do not include PII in the description of the breach report or attached documents containing PII. Reports will be forward using the DoW Defense Privacy Information Management System (DPIMS) at https://dpims.disa.mil/eCasePortal/Home.aspx. **(T-0)**

(DELETE) 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)**

(MODIFY) 3.1.6.3. The Wings and Deltas Commander must 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 5000 individuals. The Servicing Privacy Manager must notify the DAF Privacy Officer immediately upon discovery. **(T-1)**

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

command and simultaneously notify the MAJCOM by official unencrypted e-mail (Non-Classified Internet Protocol Router Network) attaching the Preliminary PII Breach Report and submitting the breach in DPIMS. This includes a breach in any medium or form, including paper, oral, and electronic. **(T-1)**

(MODIFY) 3.1.6.5. Within 24 hours of being notified of the PII breach, the MAJCOM Privacy Manager must notify the DAF Privacy Office by submitting the Preliminary PII Breach Report in DPIMS at https://dpims.disa.mil/eCasePortal/Home.aspx. **(T-1)**

(MODIFY) 3.1.6.6. Within 48 hours of the PII breach notification the DAF Privacy Officer reviews the breach report in DPIMS and submits it to the Privacy, Civil Liberties and Transparency Directorate through DPIMS. **(T-0)**

(MODIFY) 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 to the DAF Privacy Office in accordance with these reporting procedures. **(T-0)**

(MODIFY) 3.1.6.8. Upon resolution, the Privacy Manager servicing must submit the final PII Breach Report to their next higher Privacy Office, which will complete the risk assessment in DPIMS. The final breach report must include the numbers and type(s) of affected individuals, type of PII breach and risk assessment action taken in response to the breach, to include actions taken to prevent recurrence and lesson learned. **(T-0)**

(ADD) 3.1.6.9. DAF Privacy Officer will report monthly PII breaches affecting 250 or more DoW Civilians and/or Service Members to the Defense Privacy, Civil Liberties, and Transparency Directorate to report to the U.S. Senate and House Committees on Armed Services and the U.S. Senate and House Committees on Appropriations, Subcommittees on Defense, in accordance with Section 1639 of Public Law 115-232 (codified at Section 2224 note of Title 10, U.S.C.). **(T-0)**

(MODIFY) 3.2.5. Commanders/Directors must ensure that individuals who are responsible for causing the breach to receive remedial training entitled, "DoW Personally Identifiable Information," located at https://www.cyber.mil/training.

(MODIFY) 4.2.9. Use official forms and similar tools that have been approved and published in accordance with DAFI 90-160, when collecting PII. **(T-0)**

(MODIFY) 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 DAFI 33-324, The Department of the Air Force Information Collections and Reports Management Program). **(T-0)**

(MODIFY) 4.2.12.4. Transmit informational materials or communications that contain personal information to or from personal or commercial e-mail accounts unless 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 AFMAN 41-210 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. Civilians who violate information security policy may be disciplined in accordance with DAFI 36-148, Discipline and Adverse Actions of Civilian Employees. **(T-0)**

(MODIFY) 4.4.4. In accordance with 44 USC § 3501, an OMB control number must be requested whenever information is 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 DAFI 33-324). **(T-0)**

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

(DELETE) 4.5.3. Label: Department of the Air Force Visual Aid (AFVA) 33-276, Department of the 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 (D)AFI 33-322, Records Management and Information Governance Program. **(T-1)**

(MODIFY) 4.6.1. A SORN is required when personal information is maintained on an individual and is regularly retrieved by a name, number (DoW ID number, Social Security number, etc.), symbol, or other identifying (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 three types of SORN Action requests (new, modification, and rescindment) that can be submitted.

(MODIFY) 4.6.6. Submitting SORNs for publication in the Federal Register. The Program/Project Manager must submit the proposed SORN to their MAJCOM Privacy Manager at a minimum of 180 days before the planned implementation date of a new SOR or a change to an existing SOR subject to this instruction. The Privacy Manager must review for accuracy and completeness and send electronically to the DAF Privacy Office at DAF.Privacy@us.af.mil. The DAF Privacy Office must review and forward to Defense Privacy, Civil Liberties, and Transparency Directorate for review and publishing in the Federal Register. **(T-1)**

(MODIFY) 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 DoW 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 DAF Privacy Office at DAF.Privacy@us.af.mil, to forward to the Defense Privacy and Civil Liberties Directorate to have the SORN deleted from the Federal Register. **(T-1)**

(MODIFY) 4.13. Computer Matching. Computer matching programs electronically compare records from two or more automated systems, one from the DoW 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. In all cases, Computer Matching Agreements are processed by the PCLD as specified in DoW 5400.11–R and approved by the Defense Data Integrity Board. Agreements are conducted in accordance with the requirements of 5 USC § 552a and OMB Circular A–130. For additional information regarding the computer matching publication and review requirements, see DoW 5400.11–R.

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

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

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

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

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

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

(DELETE) 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:

(DELETE) 4.13.2.1. Determines Federal benefit eligibility.

(DELETE) 4.13.2.2. Checks on compliance with benefit program requirements; or

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

(DELETE) 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.

(DELETE) 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)**

(DELETE) 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 Privacy Manager and AF Privacy Officer. **(T-0)**

(MODIFY) 5.2.2. 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. The Act requires the Department of the Air Force to make PIAs publicly available, except when an agency in its discretion determines publication of the PIA would raise security concerns, reveal classified (i.e., national security) information, or sensitive (e.g., potentially damaging to a nation's interest, law enforcement effort or competitive business interest contained in the assessment) information. The Department of the Air Force PIA can be viewed at https://www.privacy.af.mil/Home/PIA/.

(MODIFY) 5.2.3.4. When the PIA is submitted to the DAF Privacy Officer, it must contain the eMASS, ITIPS and DITPR number if applicable and 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) and system artifacts. Note, a PCIL is not needed if a system does not contain PII. Additional resources on determining the PCIL can be found at the DAF Privacy SharePoint site: https://usaf.dps.mil/sites/13057/Office-of-the-CISO/CNZA/Privacy_Civil_Liberties/SitePages/Home.aspx.

MODIFY) 5.2.3. PIAs must be submitted 180 days from the scheduled operational or expiration date of the Authorization to Operate or Interim Authorization to Operate on all new and existing systems. **(T-0)**

(MODIFY) 5.2.4. The ISO must conduct a PIA in conjunction with the Authorizing Official (AO), Program Manager/Project Manager, Information System Security Managers and Servicing Privacy

Manager/Monitor. **(T-0)**

(DELETE) 5.2.5. 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)**

(DELETE) 5.2.6. All DoD Medical Department IT systems purchased with DHA funds must be reported to the DoD Information Technology Portfolio Repository via the Component Defense Health Agency (DHA). **(T-0)**

(MODIFY) 5.2.7. Format and Digital Signatures. PIAs must be completed on DD Form 2930, Privacy Impact Assessment (PIA), as an unsecured fillable PDF which requires digital signatures. The DD2930 must be signed by a government employee for accountability purposes.

(MODIFY) 5.2.8.1.1. The system Program/Project Manager or designee will digitally sign Section 4a and forward the signed PIA to their perspective ISSM/ISSO. **(T-0)**

(MODIFY) 5.2.8.1.2. Information Systems Security Managers digitally sign and forward the signed PIA to their Base Privacy Manager. Base Privacy Managers review and coordinate with the applicable records management professional to ensure appropriate lifecycle management. Generate, capture, maintain, use, preserve, and dispose of records in accordance with *DoWI 5015.02, DoD Records Management Program* and Department of the Air Force. Administration approved records schedules, and the Department of the Air Force Records Disposition Schedule. Records managers annotate in section 1, part l, of the DD 2930, "Records maintenance is consistent with National Archives and Records Administration schedule." Records managers review/coordinate and return the PIA to the PM. PMs forward the signed PIA to their respective MAJCOM Privacy Office. The MAJCOM Privacy Manager review/sign if applicable and forward the PIA to DAF Privacy Officer for review/final processing at DAF.Privacy@us.af.mil. Air Force Installation and Mission Support Center Privacy Office will sign as a reviewer of base/unit/local level PIAs in Section 4c. **(T-1)**

(MODIFY) 5.2.8.1.3. The DAF Privacy Officer must digitally sign section 4d and forward the signed PIA to the Department of the Air Force Chief Information Officer or representative through Headquarters Department of the Air Force ETMS2. **(T-1)**

(MODIFY) 5.2.8.1.4. The DAF Senior information Security Officer, Senior Component Official for Privacy and Component Chief Information Officer or representative must digitally sign section 4f - h and return PIA to the DAF Privacy Officer through the Headquarters Department of the Air Force ETMS2. **(T-1)**

(DELETE) 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)**

(MODIFY) 5.2.8. DAF Privacy Officer maintains a copy of all approved PIAs on the DAF Privacy public access website https://www.privacy.af.mil/Home/PIA/. An electronic copy will be forwarded by the DAF Privacy Officer to the Department of War Chief Information Officer (DoW CIO).

(MODIFY) 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 the DAF Privacy Officer. Submit items to appropriate Forms Manager in accordance with DAFI 33-360. **(T-1)**

(DELETE) 6.5. Reporting Results of Social Security Number Reduction.

(DELETE) 6.5.1. New Departmental Forms. The DAF Departmental Forms Management Officer shall

maintain a database to produce an annual report every July 1st. The annual report shall contain the following elements:

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

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

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

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

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

(DELETE) 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)**

(DELETE) 6.5.1.7. Existing Departmental Forms. The DAF 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:

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

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

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

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

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

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

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

(DELETE) 6.5.1.8. For existing forms issued below departmental level (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 DAF level. **(T-1)**

(MODIFY) 7.2. Protecting Personal information or PII Maintained in an Electronic System. It is DAF policy that personal information or PII collected, maintained, and stored in an electronic system must 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 DAFI 17-130, and DoWI 5400.16).

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

(MODIFY) 7.3.1. Paper or electronic documents and/or materials that contain personal information such as a recall rosters, personnel rosters, lists or spreadsheets must be marked “CUI” (See DoWI 5200.48 Controlled Unclassified Information (CUI)) (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)**

(MODIFY) 7.3.2. All paper documents and printed materials that contain personal information must be covered with the DAF Form 3227, Privacy Act Cover Sheet or a SF901 CUI Coversheet to protect PII from being viewed by unauthorized personnel when downloaded or removed from their System of Records or approved storage location. **(T-0)**

(MODIFY) 8.1. **Civil Liberties.** Civil liberties are fundamental rights and freedoms enjoyed by all individuals that cannot be restricted or deprived, without due process. Due process requires that these liberties can only be curtailed for a proper governmental objective, and the affected individual must be given notice of the proposed restriction or deprivation, and an opportunity to argue before a neutral decision maker that the civil liberties should be preserved.

(MODIFY) 8.3. Civil Liberties Annual Report.

(MODIFY) 8.3.1. The DAF Civil Liberties Officer will submit the annual report to Defense Privacy, Civil Liberties, and Transparency Directorate in accordance with DoWI 5400.11. (See Attachment 8). Annual reports are on a fiscal year schedule and are due in October to the Defense Privacy, Civil Liberties, and Transparency Directorate. **(T-0)**

(DELETE) 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 protection for asylum seekers. http://www.dhs.gov/xlibrary/assets/training/xus/crcl/asylumseekers/index.htm.

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

Prescribed Forms
(DELETE) AF Form 3227, Privacy Act Cover Sheet