BY ORDER OF THE SECRETARY OF THE AIR FORCE

HEADQUARTERS OPERATING INSTRUCTION 33-19

27 OCTOBER 2020

Communication and Information

PRIVACY PROGRAM ROLES AND RESPONSIBILITIES

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Headquarters Air Force Publications and forms are available on Air Force e-Publishing (**http://www.e-publishing.af.mil/**) under Departmental: Special Publications: HOI.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: SAF/AAII

Certified by:SAF/AAI
(Ms. Anna Santos DeDios)

Supersedes: HOI33-19, 19 June 2018

Pages: 24

This Headquarters Operating Instruction (HOI) implements the Department of Defense (DoD) 5400.11-R, *Department of Defense Privacy Program*, Air Force Policy Directive (AFPD) 33-3, *Information Management*, Air Force Instruction (AFI) 33-332, *Air Force Privacy and Civil Liberties Program*, AFI 33-324, *The Air Force Information Collections and Reports Management Program*, AFI 17-130, *Cyber Security Program Management*, AFI 17-110, *Air Force IT Portfolio Management and Capital Planning and Investment Control*, and Air Force Manual (AFMAN) 17-1301, *Computer Security (COMPUSEC)*. The purpose of this instruction is to establish and describe the duties and responsibilities of the Information Management Directorate (SAF/AAI) Privacy Manager and Unit Privacy Managers or Monitors under the oversight of the Director, Information Management, and the two- letter (2-ltr) Offices of Primary Responsibility (OPR) in regards to the Headquarters Air Force (HAF) Privacy Program. This Instruction applies to all civilian employees, military members, and contractors assigned to the HAF (Secretariat, Air Staff, Space Staff, their FOAs and AF elements). This instruction also ensures 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. Send recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) at **SAF.AA.HAF.PRIVACY.OFFICE@us.af.mil** using the AF Form 847, *Recommendation for Change of Publication*. This publication may not be supplemented.

SUMMARY OF CHANGES

This document has been substantially revised and needs to be completely reviewed. Major changes in the rewrite covers changes to roles and responsibilities to be performed by Unit Privacy Managers and Unit Privacy Monitors (UPMs), SAF/AAI Privacy Manager, Program Managers (PM), Information System Security Manager (ISSM), Information System Owners (ISO), and HAF organizations executing the Privacy functions. The rewrite also emphasizes realignment and level of support of Unit Privacy Managers or Unit Privacy Monitors for each organization's Information Technology (IT) portfolio and compliance.

1. Overview.

1.1. The HAF Privacy Program ensures the collection, maintenance, use, and dissemination of Personally Identifiable Information (PII) about individuals and the protection of individuals' rights against invasion of personal privacy is conducted in accordance with (IAW) the Privacy Act of 1974, 5 U.S.C. § 552a, Records Maintained on Individuals, and DoD policies, such as DoDI 5400.11, *DoD Privacy and Civil Liberties Programs*, and DoD 5400.11-R, Department of Defense Privacy Program. The Privacy Act focuses on four policy objectives:

1.1.1. To restrict disclosure of personally identifiable information records maintained by agencies.

1.1.2. To grant individuals increased rights of access to agency records maintained on themselves.

1.1.3. To grant individuals the right to seek amendments of agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely, or complete.

1.1.4. To implement the code of "Fair Information Practices", which requires agencies to comply with statutory norms for collection, maintenance, use, and dissemination of records.

1.2. All Air Force military, civilian, and contractor personnel are to comply with the requirements and practices governing the collection, maintenance, use, and dissemination of PII maintained by Federal agencies IAW the E-Government Act of 2002, Pub. L. 107-347, 44 U.S.C. § 101and Privacy Act of 1974, as appropriate.

2. Responsibilities.

2.1. IAW AFPD 33-3 and AFI 33-332, the office of the Deputy Chief Information Officer (SAF/CN) establishes procedures to ensure compliance with the Privacy Act and the DoD Privacy Program. In addition, SAF/CN appoints the Senior Component Official for Privacy and the Air Force Privacy Officer.

2.2. The Air Force Privacy Officer administers the program for the Air Force and performs the duties and functions outlined in AFI 33-332.

2.2.1. Individual HAF 2-ltr organizations are responsible for the implementation, oversight and management of the Privacy Program.

2.2.1.1. HAF 2-Ltr organizations UPMs help implement the Air Force Privacy Program IAW AFI 33-332.

2.2.2. Consistent with responsibilities for Air Force Information Technology (see AFI 17-110 attachment 7) and HAF Mission Directive 1-6, *Administrative Assistant to the Secretary of the Air Force*, the Information Management Directorate (SAF/AAI) is responsible for the leadership and oversight for HAF Information Resource Management, to include the Privacy Act, Freedom of Information Act, and Records Management activities (see **para 2.2.2.1** to **para 2.2.2.22**). SAF/AAI Privacy Manager will function as the Privacy subject matter expert (SME) for the following 2-ltr organizations that are part of the "HAF Command Portfolio" (see **Figure 2.1**) under the oversight of SAF/AAI (also known as blue organizations):

2.2.2.1. Auditor General (SAF/AG)

2.2.2.1.1. Air Force Audit Agency (AFAA)

2.2.2.2. General Counsel (SAF/GC)

2.2.2.3. International Affairs (SAF/IA)

2.2.2.4. Inspector General (SAF/IG)

2.2.2.4.1. Air Force Office of Special Investigations (AFOSI)

2.2.2.4.2. DoD Cyber Crime Center (DC3)

2.2.2.4.3. Air Force Inspection Agency (AFIA)

2.2.2.5. Legislative Liaison (SAF/LL)

2.2.2.6. Public Affairs (SAF/PA)

2.2.2.6.1. Air Force Public Affairs Agency (AFPAA)

2.2.2.7. Manpower & Reserve Affairs (SAF/MR)

2.2.2.7.1. Air Force Review Board Agency (AFRBA)

2.2.2.8. Air Force Office of Small Business Programs (SAF/SB)

2.2.2.9. Judge Advocate General (AF/JA)

2.2.2.9.1. Air Force Legal Operations Agency (AFLOA)

2.2.2.10. Chief of Chaplains (AF/HC)

2.2.2.11. Air Force History & Museums Programs (AF/HO)

2.2.2.11.1. Air Force Historical Research Agency (AFHRA)

2.2.2.12. Chief of Air Force Reserve (AF/RE)

2.2.2.13. Chief of Safety (AF/SE)

2.2.2.13.1. Air Force Safety Center (AFSEC)

2.2.2.14. Test and Evaluation (AF/TE)

2.2.2.15. Chief Scientist (AF/ST)

2.2.2.16. Office of the Assistant Secretary of the Air Force for Space Acquisition and Integration (SAF/SP)

2.2.2.17. Executive Secretariat (HAF/ES) to include Office of the Secretary of the Air Force (SECAF), Under Secretary of the Air Force (SAF/US), Chief of Staff of the Air Force (CSAF), Vice Chief of Staff, Assistant Vice Chief of Staff/Director of Staff (AF/CVA), and Chief Master Sergeant of the Air Force (CCC)

2.2.2.18. Installations, Environment and Energy (SAF/IE)

2.2.2.19. Management and Deputy Chief Management Office (SAF/MG)

2.2.2.20. Administrative Assistant (SAF/AA)

2.2.2.21. Air Force Integration Office (AF/IO)

2.2.2.22. Strategic Deterrence and Nuclear Integration (AF/A10)

2.2.3. The following HAF organizations with delegated responsibilities (**para 2.2.3.1** to para 2.2.3. 11), consistent with responsibilities for Air Force Information Technology (see AFI 17-110 attachment 7) may appoint a Unit Privacy Manager or Monitor (UPM) to implement the AFI 33-332, who will serve as the Privacy SME for their respective portfolio (see **Figure 2.1**) (also known as yellow organizations).

2.2.3.1. Manpower, Personnel and Services (AF/A1)

2.2.3.2. Intelligence, Surveillance, Reconnaissance, and Cyber Effects Operations (AF/A2/6)

2.2.3.3. Operations (AF/A3)

2.2.3.4. Logistics, Engineering and Force Protection (AF/A4)

2.2.3.5. Plans and Programs (AF/A8)

2.2.3.6. Office of the Secretary of the Air Force Deputy Chief Information Officer (SAF/CN)

2.2.3.7. Studies, Analyses, and Assessments (AF/A9)

2.2.3.8. Acquisition (SAF/AQ)

2.2.3.9. Financial Management and Comptroller (SAF/FM)

2.2.3.10. Surgeon General (AF/SG)

2.2.3.10.1. Air Force Medical Services Agency (AFMSA)

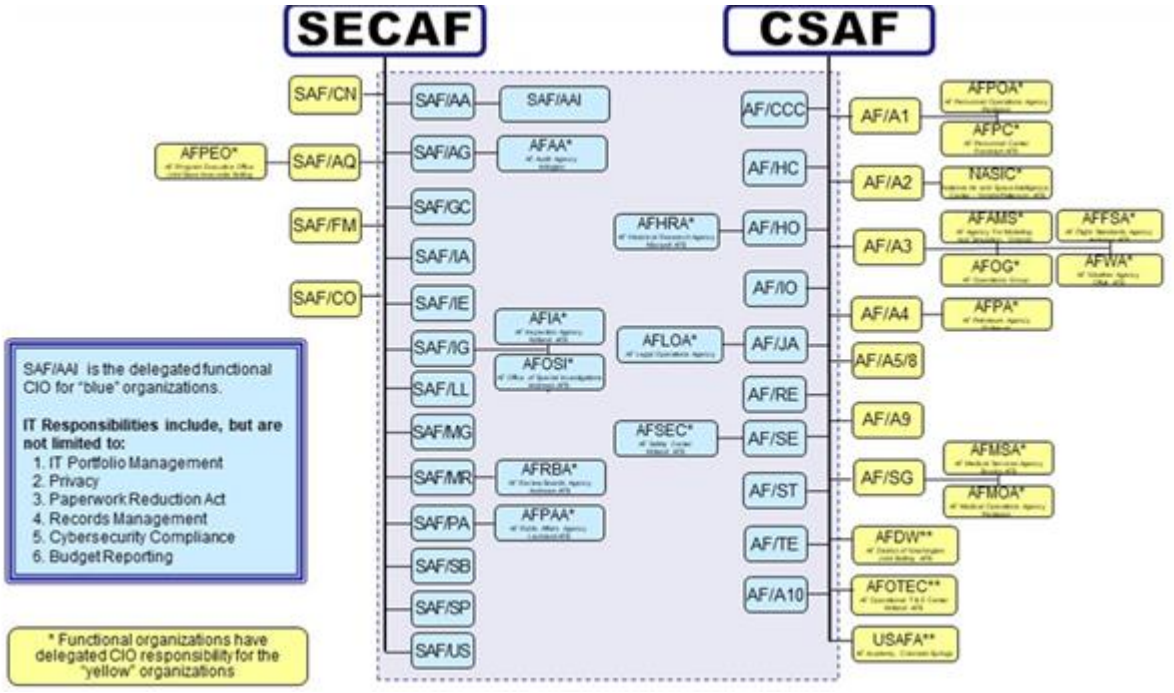
2.2.3.11. The Air Force Chief Data Office (SAF/CO)

2.3. The SAF/AAI Privacy Manager will:

2.3.1. Provide general guidance and training to Unit Privacy Managers or Monitors.

2.3.2. Serve as the HAF Command Portfolio SME and work with the HAF IT portfolio management team to ensure information systems are in compliance with Privacy Act, E-Government Act and Paperwork Reduction Act (PRA) as annotated in Information Technology Investment Portfolio Suite (ITIPS). For more information, please refer to AFI 17-110.

Figure 2.1.



2.3.3. Assist the HAF Command Portfolio's IT investment PM and ISO during development, implementation, revision, or submission of: System of Records Notices (SORNs); Paperwork Reduction Act submission packages for public information collections; DD Form 2936, Request for Approval of Department of Defense Internal Information Collections; DD Form 2930, Privacy Impact Assessment (PIA); Privacy Act Statement (PAS), and Privacy Act Advisory (PAA), PII Confidentiality Impact Level (PCIL) worksheet and Social Security Number (SSN) Justification Memo.

2.3.4. Participate in regular system reviews with HAF Command IT portfolio management team.

2.4. The Unit Privacy Managers or Monitors shall:

2.4.1. Be appointed in writing by commander or director (or designated representative) to implement the responsibilities outlined in AFI 33-332. A primary and alternate privacy monitor should be appointed (see **Attachment 2** for a sample appointment letter).

2.4.2. Complete required UPM's training within 60 days of appointment.

2.4.3. Report PII breaches and violations to the appropriate Privacy Manager, IAW AFI 33-332 and Counter-Insider Threat Program (C-InTP) representative, IAW AFI 16-1402, *Counter-Insider Threat Program Management.*

2.4.4. Administer appropriate Privacy training to members of the organization and track IAW this instruction.

2.4.5. Comply with biennial staff assistance visit by utilizing HAF checklists.

2.4.6. Provide guidance and direct support to organization's PMs, ISSM, or ISO to ensure privacy compliance is met for IT investments IAW statutory guidance. Serve as the unit's Privacy SME and work with the organization's IT portfolio management team to ensure information systems comply with Privacy Act, E- Government Act and Paperwork Reduction Act as annotated in ITIPS. For more information, please refer to AFI 17-110.

3. Procedures.

3.1. Protection of PII

3.1.1. Privacy Act records shall be:

3.1.1.1. Marked in AFRIMS inventory of records and labeled with appropriate markings when stored in Electronic Records Management (ERM) drives or other designated records repository IAW AFI 33-322.

3.1.1.2. Marked appropriately. Legacy material marked "FOR OFFICIAL USE ONLY" and "Controlled Unclassified Information (CUI)" must be protected and accessible only by those with a lawful government purpose and the official need to know. The Air Force CUI Program does not require the remarking of legacy CUI documents. However, any new document created with information derived from legacy FOUO PII material must me marked as CUI.

3.2. Electronic Storage of PII

3.2.1. PII in SharePoint and Shared Drives. Per SAF/AAI memo, *SharePoint and Shared Drives PII Cleanup*, dated 25 June 2019, information owners must conduct self-audits of their holdings on a regular basis. Unit Privacy Managers or Monitors should conduct monthly spot inspections of SharePoint and shared drives, and inappropriately exposed data will be reported as a PII breach to the owning 2-Ltr organization Unit Privacy Manager or Monitor. Exposed PII Data will also require a determination be made by the information owner as to if an inquiry/investigation is necessary. If there was a release/unauthorized disclosure of PII in the public domain or to an unauthorized person or persons resulting in administrative action, referral for criminal and/or Counterintelligence Investigation (CI), and/or resulted in suspension or revocation of clearance, then SAF/AAZ must be notified at **AAZ.Workflow@us.af.mil**.

Follow additional instructions in AFI 33-332. Spot inspections will be an interest item in the HAF staff assistance visit checklist.

3.2.1.1. Apply required safeguards (encrypted or password protected) to controlled unclassified information on SharePoint and Shared Drives or similar web base applications, or remove when no longer needed for daily operations and properly file in accordance with Air Force Records Disposition Schedule (AF RDS).

3.2.1.2. The storing of any controlled unclassified information on SharePoint and shared drives is permissible, provided the user adheres to the established Records Disposition Schedule, the Privacy Act (System of Records Notice, SSN Justification Memorandum (if applicable)), and E-Government Act of 2002; AFGM2020-16-01, *Controlled Unclassified Information* and user access is restricted to individuals with a need-to-know to conduct daily operations. Follow additional instructions in AFI 33-332.

3.2.2. PII use in Air Force Cloud Hosted Enterprise Services (CHES) Teams and DoD Commercial Virtual Remote (CVR). Refer to DoDI 5200.48, *Controlled Unclassified Information* and AF Deputy Chief Information Officer Memorandum, titled "*Department of the Air Force Telework Cyber Environment*, dated 13 April 2020, located at AF Telework Capabilities and Resources SharePoint Online, **https://usaf.dps.mil/sites/13057/sc/tcr/sitepages/home.aspx** for additional information on approved tools while teleworking.

3.2.2.1. The Air Force CHES collaboration capabilities is part of Microsoft O365 collaboration suite solution, consisting of tools such as Teams, Exchange Online, SharePoint Online, OneDrive and Microsoft Office products. CHES Teams is the version of Teams that most AF users are familiar with and is the AF's primary Microsoft O365 service. CHES Teams Collaboration tool provides users with a cloud security Impact Level 5, which is accredited for ALL CUI (no exceptions) data.

3.2.2.2. Requires both VPN connection & CAC to access CHES environment

3.2.2.3. CHES Teams provides normal operational communication and collaboration services.

3.2.2.4. CHES Teams provides permanent collaboration capability in the AF.

3.2.3. The DoD Commercial Virtual Remote (CVR) environment was specifically developed by the DoD CIO Cloud Computing Program Office (CCPO) in response to the COVID-19 National Emergency Declaration. CVR provides users with a temporary Microsoft O365 collaboration suite solution, consisting of tools such as Teams, SharePoint, Word, Excel, PowerPoint and Microsoft OneDrive cloud storage capability. CVR has been approved for the following types of controlled unclassified data: a) Non Critical Mission Essential Information and b) Low Impact PII (other types are not permitted). The DoD CIO Temporary Exception to Policy (TEP) is the authoritative source for which types of data may be stored and processed in the CVR environment. Please refer to DoD memorandum titled, "*Authorized Telework Capabilities and Guidance*", dated 13 April 2020. Refer to NIST 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* for definition of low impact PII.

3.2.3.1. CVR can be accessed from any device, both personal and/or government-issued computers and mobile devices.

3.2.3.2. Does not require VPN connection or CAC to access.

3.2.3.3. Provides temporary audio, video, virtual meetings, screen share, document collaboration and storage.

3.2.4. PII in personal laptop or device. Individuals shall not place Department of Defense Controlled Unclassified Information, except for an individual's own or minor child's Privacy Act protected information, on a personal device except as part of a SAF/CN approved Bring Your Own Approved Device (BYOAD) program. Refer to AFMAN 17-301, *Computer Security* (COMPUSEC).

3.3. PII Breach Reporting Procedures for organizations.

3.3.1. PII breach reporting flow varies within HAF.

3.3.1.1. Unit Privacy Managers or Monitors assigned to **para 2.2.2** will obtain a tracking number from and will report PII breaches directly to the SAF/AAI Privacy Office.

3.3.1.2. Unit Privacy Managers or Monitors assigned to **para 2.2.3** will assign their own tracking number and will report PII breaches directly to the AF Privacy Officer, **daf.privacy@us.af.mil** and courtesy copy SAF/AAI Privacy workflow office at **SAF.AA.HAF.PRIVACY.OFFICE@us.af.mil**

3.3.1.3. The information security officer and PM of the application or system from which the breach occurred, must notify the privacy SME of the PII breach. The Unit Privacy Manager or Monitor who serves as the privacy SME for the respective portfolio shall make appropriate breach notifications established by AF policy and DoD reporting guidance, including reporting the breaches to the Air Force C-InTP.

3.3.1.4. A PII breach and/or an unauthorized disclosure should be reported through Privacy channels as well as CUI channels.

3.3.2. PII Breach Inquiry.

3.3.2.1. Senior leaders may appoint in writing an investigating official (IO) for unique or major PII incidents IAW AFI 33-332. The IO shall:

3.3.2.2. Submit the IO report (see **Attachment 5** for a report template) to the senior official (GS-15, O-6 or higher) who is in the chain of command for approval after the inquiry. For reports on Privacy Act complaints, use the sample format in **Attachment 6** of this instruction.

3.3.2.3. Consult with their legal support office as necessary.

3.3.2.4. Submit the approved IO report to the SAF/AAI Privacy Manager through the Unit Privacy Manager or Monitor.

3.3.2.5. Refer to the HAF Privacy IO Trifold for additional instructions, see link:

https://usaf.dps.mil/sites/HAFCIO/privacy/PRIVACY%20TRIFOLDS%20AND%20VISUAL%20AIDS/Forms/AllItems.aspx?viewpath=%2Fsites%2FHAFCIO%2Fprivacy%2FPRIVACY%20TRIFOLDS%20AND%20VISUAL%20AIDS%2FForms%2FAllItems.aspx

3.4. PII Breach Response Plan for Major Incident. Per Deputy Secretary of Defense Memorandum, Reporting of Breaches of Personally Identifiable Information IAW the Department of Defense Breach Response Plan, dated 30 Nov 2018, the DoD reporting process is to be used when there is a known or suspected loss of DoD personally identifiable information. Contact the AF Privacy Office for AF specific breach response plan. If there was a release of PII in the public domain or to an unauthorized person or persons resulting in administrative action, referral for criminal and/or CI investigation, and/or resulted in suspension or revocation of clearance, then SAF/AAZ, **SAF.AAZ.Workflow@us.af.mil**, must be notified.

3.5. Loss of Account Access as a Result of PII Breaches.

3.5.1. Privacy Act protected information and PII (moderate and high) must be protected in transit and at rest with strong encryption IAW AFI33-332, AFI17-130, AFMAN17-1301, and OMB Circular A-130. Refer to AFGM2020-16-01 for handling and safeguarding of CUI. Violation will be processed as a PII breach.

3.5.2. Users may immediately and/or temporarily lose account access when user's conduct results in failure to protect high impact PII.

3.5.3. For repeat PII breach incidents, the violator's account may be disabled. IAW

AFI33-332, personnel who fail to safeguard PII may receive administrative or disciplinary action by the commander or director as appropriate.

3.5.4. The SAF/AAI Privacy Manager may notify the senior official (GS-15, O-6 or higher) in the chain of command assigned to HAF Command Portfolio of any repeated user-involved incidents.

3.5.4.1. To restore account access, the following actions must be accomplished:

3.5.4.2. The user responsible for the PII breach must complete remedial Privacy training.

3.5.4.3. The user's HAF 2-ltrd director or designated representative (GS-15, O-6 or higher) shall verify the user's completion of remedial training before signing reinstatement memo. The reinstatement memo should be addressed to the appropriate organization handling the user account through the appropriate Privacy Manager. See **Attachment 7** for a sample reinstatement memo.

3.6. IT Systems Compliance.

3.6.1. Privacy SME will evaluate IT investments to ensure compliance in Privacy Act, Paperwork Reduction Act, and E-Government Act. The assessment of IT investments under the HAF portfolio will be documented using the DD Form 2930, Privacy Impact Assessment (PIA).

3.6.1.1. During the assessment, the Privacy SME will review additional documentation (i.e. PCIL Worksheet, SORN, and SSN Justification Memo) from the PM that shows how PII impact level is determined. IAW AFI 17-101, Risk Management Framework (RMF) for Air Force Information Technology (IT), the PM will digitally sign the PIA.

3.6.1.2. The ISO/ISSM/PM submits the PIA to the assigned ISSM or other designated personnel authorized to sign on behalf of the ISSM. After reviewing the privacy overlay and ensuring e-MASS entry is valid, the ISSM or other designated personnel will digitally sign the PIA and will submit to Privacy SME for signature. Note: The SAF/AAI Privacy Manager serves as the Privacy SME for HAF Command Portfolio.

3.6.1.2.1. After the HAF Command Portfolio Privacy SME reviews and approves the privacy impact assessment documents, the impact level documented in PCIL worksheet will be reported to SAF/AAI Cyber Team.

3.6.1.3. Refer to HAF PIA guide on how to complete a DD Form 2930. Refer to HAF Portfolio PM Trifold for additional instructions at **https://usaf.dps.mil/sites/HAFCIO/privacy/default.aspx**.

3.6.2. The PCIL will be assessed based on NIST 800-122 for IT assets (such as information systems, enclave, network, application, etc.) and will be documented using the PCIL worksheet. For IT assets hosted on the cloud environment, the impact level (IL) will be assessed based on Department of Defense Cloud Computing Security Requirements Guide.

4. Training.

4.1. Initial and Annual Privacy Training Requirements.

4.1.1. Personnel must complete all required Privacy training within 60 days of assignment to HAF and thereafter annually, as necessary. Upon dissemination of CUI training from Center for Development of Security Excellence (CDSE), personnel will also be required to complete initial and annual training for CUI. Refer to AFGM2020-16-01 for more information.

4.1.2. All user Initial/Orientation and Annual Refresher Training includes:

4.1.2.1. Familiarization of Privacy practices and statutes presented through review of visual aids and PII tri-fold.

4.1.2.3. Completion of AF and/or DoD required training, such as locally devised training or any other means, as applicable.

4.1.2.4. The annual all users' Privacy training completed by supported organizations should be tracked using the HAF SharePoint training tracker at **https://usaf.dps.mil/sites/HAFCIO/privacy/trgtracker/SitePages/Home.aspx**

4.1.3. Initial and Annual Specialized Training includes:

4.1.3.1. Advanced knowledge of Privacy requirements for individuals or managers who maintain a System of Records (SORs) or manage PII on a regular basis. Specialized training is required on an annual basis. Personnel who may manage PII on a regular basis includes but are not limited to: knowledge operations managers, human resource specialists or other employees who perform military or civilian personnel management functions or duties. Security managers, law enforcement, IT personnel (programmers/developers, system administrators, SharePoint site owners, etc.), information system owners and program managers of a SOR and/or IT

investment are also required to complete the specialized training. Also needing specialized training are Freedom of Information Act analysts, records professional, personnel who may be expected to deal with the news media or the public, supervisors or other personnel who handle performance reviews or appraisals of military and civilian employees (to include branch chiefs, division chiefs, directors). Finally, individuals working with medical, personnel management, legal, general counsel, financial, and Unit Privacy Managers or Monitors, and other personnel responsible for carrying out functions under this instruction are required to complete specialized training. As a minimum, personnel must:

4.1.3.2. Familiarization of HAF Privacy practices presented through review of visual aids located at **https://usaf.dps.mil/sites/HAFCIO/privacy/default.aspx**.

4.1.3.3. Completion of Defense Information Systems Agency (DISA) CBT titled, "Identifying and Safeguarding PII", **https://dl.cyber.mil/trn/online/personally-identifiable-information-pii/launchPage.htm**.

4.1.3.4. The annual Specialized training completed by supported organizations should be tracked using the HAF SharePoint training tracker at **https://usaf.dps.mil/sites/HAFCIO/privacy/trgtracker/SitePages/Home.aspx**

4.1.4. Unit Privacy Manager/Monitor's Training includes:

4.1.4.1. Completion of Privacy 101, which is a mandatory specialized training for UPMs focused on Privacy program management, as well as SORN and PIA Training, and other specialized training requirements such as DISA CBT or Paperwork Reduction Act training.

4.1.4.2. Advanced knowledge of AFI 33-332, this HOI, DoDI 5400.11, *DoD Privacy and Civil Liberties Programs*, DoD 5400.11-R, *Department of Defense Privacy Program*, OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, OMB A130, *Managing Information as a Strategic Resource*, and OMB A108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act.*

4.1.5. The Program Managers/IT Investment Owner Training includes:

4.1.5.1. Completion of SORN and PIA training, and Paperwork Reduction Act training.

4.1.5.2. Familiarization of IT compliance guidance related to Privacy Act, E-Government Act, and Paperwork Reduction Act.

4.1.5.3. Completion of DISA CBT titled, "Identifying and Safeguarding PII", **https://dl.cyber.mil/trn/online/personally-identifiable-information-pii/launchPage.htm**.

4.1.5.4. The annual Program Managers or IT Investment Owner training should be tracked using the HAF SharePoint training tracker at **https://usaf.dps.mil/sites/HAFCIO/privacy/trgtracker/SitePages/Home.aspx**

4.2. Remedial Training.

4.2.1. Users who commit a PII breach or privacy violation, will complete the remedial training within 24 hours of breach reporting.

4.2.2. Remedial Training includes:

4.2.2.1. Completion of DISA CBT titled, "Identifying and Safeguarding Personally Identifiable Information" **https://dl.cyber.mil/trn/online/personally-identifiable-information-pii/launchPage.htm**.

4.2.2.2. Reorientation and familiarization of Privacy practices and statutes presented through visual aids, PII tri-fold, other AF and DoD guidance, as applicable (specific to type of breech).

4.2.2.3. Additional training may be directed and/or administered by the SAF/AAI Privacy Manager as needed on a case-by-case basis.

4.2.2.4. The Remedial training should be tracked using the HAF SharePoint training tracker at **https://usaf.dps.mil/sites/HAFCIO/privacy/trgtracker/SitePages/Home.aspx**

ANTHONY P. REARDON
Administrative Assistant

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Title 5 United States Code, Section 552a, *Privacy Act of 1974*

Public Law 104-13, *Paperwork Reduction Act of 1995*

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

OMB Circular A-130, *Managing Information as a Strategic Resource*, 28 Jul 2016

OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, 3 Jan 2017

OMB A108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, December 19, 2014

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

DODI 5400.11, DoD Privacy and Civil Liberties Programs, 29 Jan 2019

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

DoDI 5200.48, *Controlled Unclassified Information*, 6, March 2020

DoD *Cloud Computing Security Requirements Guide*, 16 March 2017

AFI 16-1402, *Counter-Insider Threat Program Management*, 17 Jun 2020

AFI 17-110, *Information Technology Portfolio Management and Capital Planning and Investment Control*, 23 May 2018

AFI 17-130, *Air Force Cybersecurity Program Management*, 13 Feb 2020

AFI 17-101, *Risk Management Framework (RMF) For Air Force Information Technology (IT)*, 6 Feb 2020

AFMAN 17-1301, *Computer Security (COMPUSEC)*, 12 Feb 2020

AFI 33-322, *Records Management and Information Governance Program*, 23 Mar 2020

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

AFI 33-332, *Air Force Privacy and Civil Liberties Program*, 10 Mar 2020

AF Guidance Memorandum (AFGM) 2020-16-01, *Controlled Unclassified Information*, 23 July 2020

AFPD 33-3, *Information Management*, 21 June 2016

HAF MD 1-6, *Administrative Assistant to the Secretary of the Air Force*, 22 Dec 2014

Adopted Forms

AF Form 847, Recommendation for Change of Publication

DD Form 2930, Privacy Impact Assessment (PIA)

DD Form 2936, Request for Approval of Department of Defense Internal Information Collections

DD Form 2959, Breach of Personally Identifiable Information Report

Abbreviations and Acronyms AFI—Air Force Instruction

AFMAN—Air Force Manual

AFPD—Air Force Policy Directive

AFRIMS—Air Force Records Information Management System

ATO—Authority to Operate

BYOAD—Bring Your Own Approved Device

CA—Certificate Authority

CAC—Common Access Card

CBT—Computer Based Training/Tutorial

CIO—Chief Information Officer

C-INTP—Counter-Insider Threat Program

CCPO—Cloud Computing Program Office

COMPUSEC—Computer Security

CUI—Controlled Unclassified Information

CVR—Commercial Virtual Remote

DISA—Defense Information Systems Agency

DoD—Department of Defense

DoD SAFE—Department of Defense Secure Access File Exchange

ECA—Email Certificate Authority

FOUO—For Official Use Only

GO/SES—General Officer/Senior Executive Service

HAF—Headquarters Air Force

HOI—Headquarters Operating Instruction

IAW—In Accordance With

IO—Investigating Official

ISSM—Information System Security Manager

ISO—Information System Owners

IT—Information Technology

NIST—National Institute of Standards and Technology

OMB—Office of Management and Budget

OPR—Office of Primary Responsibility

PA—Privacy Act

PAA—Privacy Act Advisory

PAS—Privacy Act Statement

PIA—Privacy Impact Assessments

PCIL—Personally Identifiable Information Confidentiality Impact Level

PM—Program Manager

PHI—Protected Health Information

PII—Personally Identifiable Information

PIV—Personal Identity Verification

PM—Program Manager

RDS—Records Disposition Schedule

RMF—Risk Management Framework

SAFE—Secure Access File Exchange

SME—Subject Matter Expert

SOR—System of Records

SORN—System of Records Notice

TEP—Temporary Exception to Policy

UPM—Unit Privacy Manager or Monitor

Terms

Aggregated Information—Information elements collated on a number of individuals, typically used for the purposes of making comparisons or identifying patterns.

Common Access Card—The CAC, a "smart" card about the size of a credit card, is the standard identification for active duty uniformed Service personnel, Selected Reserve, DoD civilian employees, and eligible contractor personnel. It is also the principal card used to enable physical access to buildings and controlled spaces, and it provides access to DoD computer network and systems.

Controlled Unclassified Information—Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.

Disclosure—To give information from a system, by any means, to anyone other than the record subject.

Harm—Any adverse effects that would be experienced by an individual (i.e., that may be socially, physically, or financially damaging) or an organization if the confidentiality of PII were breached.

Individual—A living US citizen or a permanent resident alien.

IT Portfolio—A grouping of IT investments by capability to accomplish a specific functional goal, objective, or mission outcome.

Personal Identifier—A name, number, or symbol that is unique to an individual, usually the person's name or social security number.

Personal Information—Information about an individual other than items of public record.

Personally Identifiable Information—Information that can be used to distinguish or trace an individual's identity, alone or when combined with other information that is linked or linkable to a specific individual. The personally identifiable information may range from common data elements such as names, addresses, dates of birth, and places of employment, to identity documents, Social Security numbers (SSNs) or other government-issued identifiers, precise location information, medical history, and biometrics.

Personally Identifiable Information Breach—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.

PII Confidentiality Impact Level—The PII confidentiality impact level—low, moderate, or high—indicates the potential harm that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

Portfolio Management—Management of selected groupings of IT investments using strategic planning, architectures, and outcome-based performance measures to achieve a mission capability.

Privacy Act Advisory—Text that informs an individual of the reasons the Privacy Act protected information is being solicited and how it will be used.

Privacy Act Statement—Text that informs an individual of the authority, purpose, routine use, if disclosure is voluntary or mandatory, and any consequences of nondisclosure; required when soliciting personally-identifying information by an Air Force web site or form.

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

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

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

System of Records Notice (SORN) /or/ Privacy Act System Notice—Official public notice published in the Federal Register of the existence, content, and Points of Contact for the SOR containing Privacy Act data.

Attachment 2

SAMPLE APPOINTMENT OF ORGANIZATION / UNIT PRIVACY MONITORS

(Date)

MEMORANDUM FOR SAF/AAII (Privacy Manager)

FROM: (Sender Two-Letter Organization supported by HAF/CIO)

SUBJECT: Appointment of Organization / Unit Privacy Monitor

The following individuals are appointed as privacy monitor for this organization. Organization privacy monitors will monitor the Privacy Act Programs for all assigned offices and perform duties in accordance with HOI 33-19.

PRIMARY NAME:

RANK/GRADE:

OFFICE SYMBOL:

DUTY PHONE:

E-MAIL:

ALTERNATE NAME:

RANK/GRADE:

OFFICE SYMBOL:

DUTY PHONE:

E-MAIL:

Appointed monitors will complete training within 60 days from the date of this letter and will contact SAF/AAII 90 days prior to any OPR changes (ex. Permanent Change of Station or Assignment (PCS, PCA), retirement, etc.).

This letter supersedes previous letter, same subject.

Signature Block

Attachment 3

INSTRUCTIONS FOR USING DOD SECURE ACCESS FILE EXCHANGE (SAFE) AND ENCRYPTION WIZARD

A3.1. DoD SAFE: DoD SAFE is a web-based tool that provides authenticated DoD CAC users and guests (unauthenticated users) the capability to securely send and receive large files, including files that are too large to be transmitted via email. Guests can receive files from CAC users and (only if CAC users requested files) send files to CAC users. Notification is achieved via email.

A.3.1.1. Email messages with large attachments can wreak havoc on email servers and end-users' computers. Downloading such email messages can take hours on a slow Internet connection and block any sending or receiving of messages during that time. In some cases, the download will fail repeatedly, breaking the recipient's ability to receive mail at all. Also, Internet email clients add considerably to the size of the file being sent. For example, saving an Outlook message with an attachment adds up to 40% to the size of the file. To share files larger than 1MB, use DoD SAFE to temporarily make a file (or files) available to another user across the Internet, in a secure and efficient manner.

A.3.1.2. DoD Secure Access File Exchange (SAFE) has an ATO and is approved for transfer of Controlled Unclassified Information (CUI)), Personally Identifiable Information (PII), and Protected Health Information (PHI) data. DoD SAFE utilizes the latest web browser encryption transport protocols to secure files when they are in transit. Files uploaded into SAFE can be encrypted at rest if the sender selects the corresponding check box on the DoD SAFE site. DoD SAFE users are responsible for ensuring they encrypt FOUO, PII, and PHI data. DoD SAFE is for Controlled Unclassified Information (CUI).

A.3.1.3. Users should select their SIGNATURE certificate issued through the DoD Email Certificate Authority (CA) or select the AUTHENTICATION Personal Identity Verification (PIV) certificate issued by the DoD Identifier (ID) Certificate Authority (CA) in order to connect. Non-DoD Personal Identity Verification certificates or External Certificate Authority are not currently supported. DoD SAFE application can be accessed via **https://safe.apps.mil/**.

A3.2. Encryption Wizard: Information about Encryption Wizard is found in the Help Menu, manual, and the many documents (including whitepapers) found within **http://spi.dod.mil/ewizard.htm**. The Air Force Research Laboratory offers additional information about Encryption Wizard upon request.

Attachment 4

APPOINTMENT OF PRIVACY INVESTIGATING OFFICIAL TEMPLATE

DEPARTMENT OF THE AIR FORCE AIR FORCE UNIT HEADING

MEMORANDUM FOR [Name, Rank, Organization, Duty Position]

FROM: [Senior-level individual who is in the chain of command for the organization where the breach took place]

SUBJECT: Appointment of Privacy Inquiry Official—[Unit] Personally Identifiable Information Breach

This is to inform you that you are hereby appointed to conduct an inquiry into a possible breach of personally identifiable information. You task is to determine if there was a breach. If there was a breach, you need to determine the cause of the breach.

Explain the incident. "On xx May 2014, it was discovered that an email with a squadron rack and stack roster, as well as a document titled "Work Stuff & Bio" was sent from the XXX office to a personal dot-com email. The email was sent unencrypted and was detected by Privacy Act Monitor at AF/XX at the Pentagon. These individuals were identified and need to be notified of the breach by the Inquiry Official."

You are directed to meet with the Privacy Manager……., who will provide you with guidance on how to complete the PII Incident Final Report and with the AF Instructions, DoD policies and a copy of the Privacy Act to be used in completing your inquiry. You are authorized to interview personnel, take sworn statements or testimony, examine and copy any and all relevant Air Force records, files and correspondence germane to this inquiry.

Please submit a complete report to me NLT xx June 2017. You may not release any information related to this investigation without prior approval.

Signature block of Senior-level individual's who is in the chain of command for the organization where the breach took place

CONTROLLED UNCLASSIFIED INFORMATION (CUI) *When Filled In*

Attachment 5

TEMPLATE FOR PII INCIDENT REPORT

MEMORANDUM FOR HAF Privacy Office

FROM: [Senior-level individual in the chain of command for the organization where the breach took place]

SUBJECT: Preliminary Inquiry of Possible Personally Identifiable Information Breach at (unit)

Authority: A preliminary inquiry was conducted (date) under the authority of the attached memorandum.

Matters investigated: The basis for this inquiry is to determine if there was a breach at the (unit in question) (breach is defined as "possible loss of control, compromise, unauthorized disclosure, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic"). Provide a short summary of the personally identifiable information incident including the date it occurred.

Personnel Interviewed: (list all personnel interviewed, title, office symbol, and security clearance).

Facts: (list specific details answering who, what, why, where, and when questions concerning the personally identifiable information incident).

Conclusions: As a result of the investigation into the circumstances surrounding the personally identifiable information incident, interviews, and personal observations, it is concluded that: (list specific conclusions reached based on the facts and if a breach or potential compromise did or did not occur). If a damage assessment is or has been done, provide the point of contact along with: the status of the assessment if it hasn't been completed; or, describe the outcome if it has been completed; or, provide a copy of the completed assessment report.

Recommendations: (Discuss risk assessment factors; list corrective actions needed to preclude a similar incident; the category of the incident; damage assessment; if the incident is a breach, compromise, potential compromise or no compromise; and, if this inquiry should be closed without further investigation or with a recommendation for a formal investigation).

If a military member is being questioned, ensure particular rights be afforded to military members under Article 31 for any inquiry/investigation they are questioned about as a subject or responsible party. Please consult with the servicing legal office prior to the questioning of the military member.

(Signature block of inquiry official)

Appointment of Inquiry Official Memo, (date)

1st Ind, XXXXX/CC Concur/NonConcur

CONTROLLED UNCLASSIFIED INFORMATION (CUI) *When Filled In*

Attachment 6

SAMPLE PRIVACY COMPLAINT REPORT

1. Name of Official (IO) conducting the Inquiry: Rank and/or Grade:
Organization of Official: Fully identify the title of the organization and location without abbreviations. (You may include authorized abbreviations or symbols in parentheses.) Duty Position and Contact Telephone Number:

2. Headquarters Air Force (HAF) Portfolio Privacy Complaint #:

3. Summary: Identify the allegations, applicable organization and location, the person(s) or organization(s) against whom the allegation is made, scope of the investigation conducted, documents reviewed, witnesses interviewed and whether the interviews were conducted telephonically or in person. The identity of interviewees need not be reflected in the report but should be documented in the official file of the agency conducting the investigation.

4. Findings: For each allegation, state the analysis of the findings as they relate to each allegation and a brief explanation of what led to the findings. Provide a list of relevant documents and/or evidence, and witness testimony in support of the findings. If they are not filed with the field working papers, list the location of relevant documents.

5. Cite any Criminal or Regulatory Violation(s) Substantiated:

6. Disposition: For investigations involving economies and efficiencies, include any management actions taken as part of the final report. For examinations involving criminal or other unlawful acts, include the results of criminal prosecutions, providing details of all charges and sentences imposed. Include the results of administrative sanctions, reprimands, value of property or money recovered or other such actions taken to preclude recurrence. Identify what corrective action was taken based on the recommendations identified above.

7. Specify Security Classification of Information: Determine and state, when applicable, any security classification of information included in the report that may jeopardize national defense or otherwise compromise security if the contents were disclosed to unauthorized sources.

8. Location of Field Working Papers and files: (Identify where CDIs, OSI reports, etc. are stored and who the release authority is.)

9. Conclusions and Corrective Action: For each allegation, state the conclusions made by the IO. This section should also include comments as to the adequacy of existing policy or regulations, noted weaknesses in systems of internal controls, and any recommended corrective actions.

10. Statement of Impartiality: Short statement demonstrating appointed Official is independent (in both fact and appearance) from all subjects/complainants (whether persons or organizations). Add the statement: “I certify that I do not have any personal impairment to independence regarding this case.”

IO SIGNATURE BLOCK

CONTROLLED UNCLASSIFIED INFORMATION (CUI) *When Filled In*

Attachment 7

SAMPLE ACCOUNT REINSTATEMENT MEMORANDUM

MEMORANDUM FOR (624 OC NETOPS)

FROM: (Insert originating org office symbol)
SUBJECT: Request to Reinstate Account Access

1. Please release the (S)AF/XX network account of_____from quarantine.

2. I have ensured that_____has completed the required remedial Privacy Act training, including the DISA CBT - Identifying and Safeguarding Personally Identifiable Information, the review of the following local guidance: OMB M-17-12, dated Jan 2017, Department of Defense 5400.11R, AFI 33-332, HQ Air Force Visual Aids, and SAF/AA personally identifiable information Tri-Fold. Member has completed and signed a certification statement of initial/annual/remedial refresher training for Privacy Act Information.

3. Member has scanned and sent a copy of DISA CBT certificate and signed certification statement to the SAF/AAI Privacy Manager and (S)AF/XX Organization Privacy Monitor.

SIGNATURE BLOCK

(GS-15, O-6 or higher)

2 Attachments:

1. Identifying and Safeguarding Personally Identifiable Information CBT Certificate
2. Certification of Initial/Annual/Remedial Refresher Training