BY ORDER OF THE COMMANDER
SHAW AFB

AIR FORCE INSTRUCTION 33-332

SHAW AIR FORCE BASE
Supplement

31 JULY 2025

Communications and Information

AIR FORCE PRIVACY AND CIVIL LIBERTIES PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: USAF/20 CS/SCOK

Certified by: 20 CS/CC
(Lt Col Ebony D. Haney)

Supersedes: AFI33-332_SHAWAFBSUP, 9 March 2021

Pages: 4

AFI 33-332, *Air Force Privacy and Civil Liberties Program*, is supplemented as follows: This supplement establishes the policies and procedures for Privacy Act compliance within the 20 FW and associated tenant units. Adherence to the Privacy Act and protecting Personally Identifiable Information (PII) is the responsibility of every federal employee, military member, and contractor assigned to the 20 FW and associated tenant units. The wing and associated tenants will foster and maintain a culture of compliance with respect to the Privacy Act and safeguarding PII. Ensure that all records created as a result of processes prescribed in this publication are maintained IAW Air Force Instruction (AFI) 33-322, *Records Management and Information Governance Program*, and disposed of IAW Air Force Records Information Management System Records Disposition Schedule (RDS). Contact supporting records managers as required. Send comments recommended changes, and questions about this publication, on AF Form 847, *Recommendation for Change of Publication*, to 20 CS/SCOKR, 504 Shaw Drive, Suite 1046, Shaw AFB, SC 29152-5028; route through your appropriate functional chain of command. Compliance with the attachment in this publication is not mandatory.

SUMMARY OF CHANGES

Paragraphs 1.1.1.1; 2.9.4.1, 2.9.4.2; 2.12.3.1; 2.12.4.1; 2.15, 2.15.1, 2.15.1.1, 2.15.1.2; 3.2.5.1, 3.2.5.2, and 7.3.2.1 were added.

1.1.1.1. **(Added)** The primary intent of this program is to safeguard private and/or personal information. Any breach of such information requires prompt and direct action to identify the root cause, eliminate reoccurrence, and to hold the violator accountable for their actions. Commanders must be made aware of all PII breaches and will consider each PII breach on a case-by-case basis to determine appropriate action. When determining actions to be taken, commanders should assess whether the breach was inadvertent, negligent, or malicious and whether there were previous offenses.

2.9. **MAJCOM and Base Privacy Managers/Monitors shall:** The Base Privacy Act Manager shall:

2.9.4.1. **(Added)** Brief base leadership at least annually on Privacy Act and PII training completion rates.

2.9.4.2. **(Added)** Develop and maintain current training resources for use by organizational commanders and others.

2.12.3.1. **(Added)** Ensure all personnel complete Privacy Act and PII training annually. Commanders have flexibility in the format (Commander's Call briefing, computer-based training (CBT), etc.); however, all training must be reviewed and approved by the Wing Privacy Act Manager to ensure it is current and accurate.

2.12.4.1 Ensure Privacy Act and PII training completion rates are reported to the Wing Privacy Act Manager at least quarterly.

2.15. **(Added) Unit Commanders Shall:**

2.15.1. **(Added)** Appoint in writing a primary and alternate Unit Privacy Act Monitor.

2.15.1.1. **(Added)** Provide a copy of the appointment letter to the Wing Privacy Act Manager at 20 CS/SCOKR.

2.15.1.2. **(Added)** Review the appointment letter annually to ensure it is up-to-date.

3.2.5.1. **(Added)** First Offense: At a minimum, the offender and his/her immediate supervisor shall complete the PII CBT located at **https://public.cyber.mil/training/identifying-and-safeguarding-personally-identifiable-information-pii** and Cyber Security Awareness training located on the myLearning web site. The Unit Privacy Act Monitor will track and document the training in the PII breach file.

3.2.5.2. **(Added)** Second and Subsequent Offenses: At a minimum, the offender and his/her immediate supervisor shall complete the PII CBT located at **https://public.cyber.mil/training/identifying-and-safeguarding-personally-identifiable-information-pii** and Cyber Security Awareness training located on the myLearning web site. The Unit Privacy Act Monitor will track and document the training in the PII breach file. A letter signed by the member's unit commander certifying that the training has been accomplished must accompany the PII breach report sent to the group commander. Commanders must consider whether additional action is warranted.

7.3.2.1. **(Added)** 100% shredding of all paper documents or printed materials regardless of content.

KEVIN D. HICOK, Colonel, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

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

Prescribed Forms

AF Form 847, *Recommendation for Change of Publication.*

Adopted Forms

No adopted forms are added to this publication.

Abbreviations and Acronyms

CBT—Computer-Based Training

FW—Fighter Wing

PII—Personally Identifiable Information

RDS—Records Disposition Schedule

Terms

Records Disposition Schedule (RDS)—- A document providing mandatory instructions for what to do with records (and non-record materials) no longer needed for current Government business, with provision of authority for the final disposition of recurring or nonrecurring records; also called records disposition schedule, records control schedule, records retention schedule, and disposition schedule, or schedule. Includes the SF 115, GRS, and agency records schedule, that, when completed, becomes a comprehensive records schedule that also contains agency disposition instructions for non-record materials.