BY ORDER OF THE
SECRETARY OF THE AIR FORCE
(AMC)

AIR FORCE INSTRUCTION

33-332

2 NOVEMBER 2020

COMMUNICATIONS 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: 628 CS/SCXK

Certified by: 628 CS/CC
(Maj Saheba B. DeHenre)

Supersedes: AFI33-332_JBCHARLESTON SUP, 2 October 2019

Pages: 4

This supplement establishes the policies and procedures for Air Force Privacy Program compliance within Joint Base Charleston (JBCHS) and associated tenant units. Adherence to the Privacy Act (PA) and protecting Personally Identifiable Information (PII) is the responsibility of every federal employee, military member, and contractor assigned to JBCHS. The Air Force Privacy Program provides direction to safeguard against the invasion of personal privacy. We must commit to preventing the loss of control, compromise, and unauthorized disclosure of PII and PA information. JB Charleston and associated tenants will foster and maintain a culture of compliance with respect to the PA 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 in IAW Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS. Compliance with the attachment in this publication is mandatory. Contact supporting records managers as required. Send comments, recommended changes, and questions about this publication on Air Force (AF) Form 847, *Recommendation for Change of Publication*, to 628 CS/SCXK, 103 N. Graves Ave, Bldg. 302, Joint Base Charleston SC 29404; route through your appropriate functional chain of command.

2.8. **MAJCOM and Wing Commanders shall:**

2.8.1.1. **(JBCHS)** The JB Charleston installation commander will appoint a primary and alternate installation Privacy Manager/Civil Liberties point of contact (Base Privacy Manager (BPM)) in writing to the Air Force Installation & Mission Support Center (AFIMSC/IZSI) Privacy Manager. The BPM will be the OPR for the appointment memorandum and will submit an update upon change in the JB Charleston installation commander and/or appointed personnel. (See **Paragraph 2.9** of the AFI for Base Privacy Manager requirements.)

2.8.8. **(JBCHS)** Organizational Commanders/Equivalents will appoint a primary and alternate Unit Privacy Monitor (UPM) in writing and submit to the BPM (628 CS/SCXK (Privacy/Civil Liberties Manager)). Submit updated appointment upon change in the Commander/Equivalent and/or appointed personnel. (See **Paragraph 2.12** of the AFI for UPM requirements.)

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

2.9.1. **(JBCHS)** Execute base-level responsibilities as outlined in this instruction.

2.9.18. **(JBCHS)** Coordinate with the base Network Control Center (NCC) quarterly (or as needed) to ensure all base Shared Drives are scanned for unprotected PII. (See **Paragraph s 7.1.2 and 7.4** of the AFI)

2.12. **Unit Privacy Monitor shall:**

2.12.1.1. **(JBCHS)** Within 10 duty days of being appointed, attend UPM training provided by the BPM and complete Identifying and Safeguarding PII computer-based training located at **https://cyber.mil/training/identifying-and-safeguarding-personally-identifiable-information-pii/**. Provide a copy of the training certificate to the BPM.

2.12.2.1. **(JBCHS)** Upon notification delete and/or facilitate the deletion and/or proper protection of unprotected PII on the unit's Shared Drive discovered during the base NCC's Shared Drive scan for unprotected PII. Continuously promote awareness to ensure PII on Shared Drives is accessible only to individuals who official duties provide them a valid need-to-know. (See **Paragraph s 7.1.2 and 7.4** of the AFI)

2.12.3. **(JBCHS)** Keep organizational Commander/Equivalent abreast of privacy training requirements and completion rates.

2.12.3.1. **(JBCHS)** Track remedial training for individuals responsible for causing PII breach. Maintain and provide a copy of the remedial training certificate to the BPM. (See **Paragraph 3.2.5** of the AFI.)

2.12.3.2. **(JBCHS)** Privacy Training tools for use:

2.12.3.2.1. **(JBCHS)** JB Charleston Privacy Training computer-based training on the Advanced Distributed Learning Services (ADLS) Air Mobility Command (AMC) Gateway located at **https://amc.adls.af.mil/login.aspx**.

2.12.3.2.2. **(JBCHS)** Unit Privacy Training PowerPoint presentation provided by the BPM. This tool is for use by the UPM for in-person training.

2.12.4.1. **(JBCHS)** Specialized Privacy Training Tool for use: Identifying and Safeguarding PII Computer Based Training (CBT) located at **https://cyber.mil/training/identifying-and-safeguarding-personally-identifiable-information-pii/**.

2.12.6.1. **(JBCHS)** Provide guidance/assistance, as needed, on the removal of PII data on the unit's SharePoint site discovered during the SCA monthly scan of SharePoint sites. (See **Paragraph 2.8.3** of the AFI and **Paragraph 2.15.1** of this supplement.)

2.12.7. **(JBCHS)** Upon request submit Privacy Training report to the BPM. Privacy Training reports will consist of: (1) the number of personnel who completed Annual Privacy training, and (2) the percentage rate for the total number of personnel current on privacy training.

2.15. **(JBCHS) Base Site Collection Administrator (628th Communications Squadron Knowledge Management Center (KMC)) and/or Unit SharePoint Site Owner shall:**

2.15.1. **(JBCHS)** Perform a monthly scan of SharePoint sites for PII data. If PII data is discovered during the scan then delete or move to an authorized location and properly protect. The base SCA will notify the unit SharePoint site owner to delete or move PII discovered on SharePoint. The base SCA will delete PII data not deleted or moved by the unit SharePoint owner. (See **Paragraph 2.8.3** of the AFI.)

2.15.2. **(JBCHS)** Provide guidance and assistance to UPMs with performing quarterly scan of unit Shared Drives in reinforcement of the protection/safeguarding of PII. (See **Paragraph 2.12.2.1** of this supplement.)

3.1. **PII Breach Reporting:**

3.1.2.1. **(JBCHS)** The UPM/BPM upon receiving report of a potential or actual breach will ensure it is reported to the Commander/Equivalent of unit in which the breach occurred. Commanders/Equivalents will consider each potential or actual breach on a case-by-case basis to determine appropriate action. Any breach of privacy information requires prompt and direct action to identify the root cause, eliminate reoccurrence, and to hold the violator accountable for their actions. (See **Chapter 3** of the AFI for Breach Reporting.)

3.2. **Guidelines for conducting an inquiry of a PII Incident.**

3.2. **(JBCHS)** The inquiry should assess if the cause of the breach was inadvertent, negligent, or malicious and whether there were previous offenses.

Marc E. Greene, Colonel, USAF
Commander, Joint Base Charleston

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

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

Prescribed Forms

None

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

ADLS—Advanced Distributed Learning Services

AFI—Air Force Instruction

AFRIMS—Air Force Records Information Management System

BPM—Base Privacy Manager

CBT—Computer Based Training

JBCHS—Joint Base Charleston

KMC—Knowledge Management Center

OPR—Office of Primary Responsibility

PA—Privacy Act

PII—Personally Identifiable Information

RDS—Records Disposition Schedule

SCA—Site Collection Agency

UPM—Unit Privacy Monitor