

49TH WING PRIVACY ACT BREACH RESPONSE

A Personally Identifiable Information (PII) breach is defined as actual or possible loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access or any similar term referring to situations where persons other than authorized users and for another than authorized purpose have access or potential access to PII, whether physical or electronic. Examples of a PII breach are:

- Improper disposal (PII found in a dumpster)
- Stolen laptop storing PII
- Unsecure or unauthorized transmission of PII
- Accessing the records of any person when not authorized
- Unauthorized access to unsecured or unprotected PII (Shared Drives, SharePoint, ERM, etc.)

HOLLOMAN PERSONNEL: If Holloman Personnel find unsecured/unprotected PII, they must follow the procedures below:

Step 1: STOP! Secure the material containing PII! If the incident involves an e-mail containing PII that was sent mistakenly to the wrong addressee, ensure that the e-mail is **IMMEDIATELY** recalled. Contact the addressee and ask that the e-mail is deleted from their Outlook *Inbox* and deleted from the *Deleted Items* folder.

Step 2: Notify the Unit Privacy Monitor (usually the unit Functional Area Records Manager) **IMMEDIATELY**. If the Unit Privacy Monitor is unavailable, contact the Holloman Privacy Act Manager (PAM) at the Knowledge Management Center (KMC) by telephone, ext. 572-7248/7.

UNIT PRIVACY MONITOR PROCEDURES: If the Unit Privacy Monitor discovers or is notified of a PII breach, they will:

Step 1: STOP! Secure the material containing PII! If the violation involves an e-mail containing PII that was sent mistakenly to the wrong addressee, ensure that the e-mail is **IMMEDIATELY** recalled. Ensure that the addressee is contacted and asked to delete the e-mail from their Outlook *Inbox* and the *Deleted Items* folder.

Step 2: Notify the unit commander of the potential breach.

Step 3: Notify the Holloman PAM (572-7248/7247) within **ONE HOUR** of discovery.

Step 4: The unit Privacy Monitor will complete DD Form 2959, *Breach of Personally Identifiable Information (PII) Report* IAW AFI 33-332, *Air Force Privacy and Civil Liberties Program* (para 1.1.2.4.5.2), and send it to the Holloman PAM (holloman.foia@us.af.mil). Include the following:

- Brief description of incident, to include facts and circumstances surrounding the loss, theft, or compromise
- Describe actions taken to mitigate the PII incident
- Send a copy of the item involved in the breach (i.e., spreadsheet, e-mail, roster, etc.) to the Holloman PAM. **REMEMBER** to secure the item with proper PII protection before sending it to the PAM!

HOLLOMANAFBVA 33-6, 17 July 2015, (per HAFBI 33-302)

OPR: 49 CS/SCOK

Certified by: 49 CS/CC (Lt Col Brian Balazs)

Step 5: The Holloman PAM will determine if a breach has occurred (as defined by AFI 33-332).

Step 6: If it has been determined that a breach has occurred, within 24 hours, the Holloman PAM will notify the FARM, and senior official (O-6/GS-15 or higher) in the unit chain of command.

Step 7: The senior official who is in the chain of command for the unit where the breach occurred will appoint an Investigating Officer (IO) IAW AFI 33-332 (para 1.1.2.5).

Step 8: The IO will conduct an inquiry IAW AFI 33-332 (para 1.1.2.5). The appointed official may contact the Holloman PAM (572-7248) for guidance.

Step 9: Within 5 days of the completion of the inquiry, the senior official will route the final breach report (DD Form 2959) to the Holloman PAM.

Step 10: The Holloman PAM will assist the unit commander in resolving and closing the PII breach.

Transmission of PII

- Exercise caution before transmitting PII via e-mail to ensure the message is adequately safeguarded.
- PII will only be e-mailed to individuals on a need to know basis.
- Before forwarding an e-mail you have received containing PII, verify that your intended recipients are authorized to receive the information under The Privacy Act. Additionally, permission from the original sender is necessary before forwarding an e-mail containing PII.
- All e-mails that contain PII must include "FOUO" in the subject line and contain the appropriate PAS at the beginning of the body of the e-mail. This process may be automatically accomplished by using the Digital Signature Enforcement Tool (DSET) function in Outlook.
- Official e-mail containing PII shall be encrypted.
- Do not send unencrypted e-mail containing PII to distribution groups or non .mil e-mail addresses.
- PII may not be sent to unauthorized systems. Sending PII to a home computer, or any unauthorized system is not allowed.
- Some information may be so sensitive and personal that e-mail may not be the appropriate means of transmitting (see AFI 33-332, para. 2.5.6).

Training

- Commanders will ensure all assigned personnel complete the required annual training (see AFI 33-332, para. 4.6.6):
 - The Total Force Awareness Training (TFAT)
 - Specialized Training – Specific to Systems of Record
 - Management Training – Managers/Decision makers
- Commanders will also ensure that all assigned personnel complete the required training (see AFI 33-332, para. 4.6.6):
 - Newcomers Orientation Training (upon hiring)
 - Remedial Training (as needed)

Protection of SSN

- The SSN in any form, including but not limited to truncated, masked, partially masked, encrypted, or disguised SSN will be protected as High Impact PII and marked FOR OFFICIAL USE ONLY.