Headquarters U.S. Air Force

Integrity - Service - Excellence

Personally Identifiable Information (PII) Overview

Mr. LaDonne L. White
Air Force Privacy and Civil Liberties Officer

U.S. AIR FORCE

Agenda

- Privacy
- PII and E-mail
- E-mail Shortfalls
- Impacts
- What Can You Do?
- Challenges
- Commanders/Director, What Can You Do?
- Conclusions

U.S. AIR FORCE

Privacy

- How many of you have been affected by a breach of your privacy?
- How many of you had to cancel a credit card due to your card/information being stolen? Or worse?
- How many of you know of a mission being affected by a Privacy breach?

U.S. AIR FORCE

PII E-Mail Issues

- Unencrypted emails containing PII accounted for **755** out of the reported **892** breaches (**85%**) for CY17 (10 or more data elements discovered). Actual breach number consisting of 1 or more data elements over 600k.
- 47 out of the 755 reported breaches affected over 5k individuals – generating an OPREP for CSAF awareness
- Under Secretaries attention early 1st Qtr FY 18 (multiple OPREPS in two month span (51K affected))

U.S. AIR FORCE

E-Mail Shortfalls

- Sending PII unencrypted
- Sending PII to the wrong recipient
- Not checking attachments for PII (hidden data fields)
- Inadvertent loss of control
- Internal email vs. External email
  - us.af.mil to us.af.mil; us.af.mil to mail.mil; mail.mil to us.af.mil, mail.mil to mail.mil; Commercial email (.gmail, .yahoo) to us.af.mil or mail.mil
- Documents not password protected or protected on shared drives
- Documents on SharePoint w/o data-at-rest encryption (why?)

U.S. AIR FORCE

Impacts

- Mission!!!!
- Potential PII Breaches
- Identity theft
- Discrimination
- Emotional distress/physical harm
- Inappropriate denial of benefits
- Harm to reputation – Blackmail - Embarrassment
- Negative consequences for the United States Air Force (USAF), and potential legal ramifications

U.S. AIR FORCE

What Can You Do?

- Limit SSN use in any form (including the last four digits)
  - Substitute the DoD ID number or other unique identifier
  - If no need – DON'T USE IT
- Share only with those having an official need to know
- Encrypt all emails containing PII or use ARMDEC SAFE
- Password protect
- Dispose when no longer required IAW records disposition
- Notify your supervisor or privacy manager if you suspect or discover that PII has been lost or compromised
- Implement safeguards (Administrative, Technical and Physical)

U.S. AIR FORCE

What Can You Do (cont.)?

- Prevent compromise or misuse during storage, transfer or use, including working at authorized alternative worksites
- Challenge ANYONE seeking personal info in your possession
- Mark privacy records appropriately
- Collect only what is necessary to properly perform your job
- Safeguard at a level equal to the risk and degree of harm resulting from the loss, misuse, or unauthorized access
- Do not collect personal information without proper authorization
- Prevent compromise or misuse during storage, transfer or use

Be Vigilant

U.S. AIR FORCE

Challenges

- Policy changes out of our control
  - The need for Privacy Act training
  - Continual changes to OMB-DOD-AFI guidance
- Pushing the message to the field
  - Commanders roles/responsibilities regarding PII
    - Do you know your Privacy POCs?
    - Are Commanders asking the right questions regarding breaches?
    - Are we efficient during a potential breach investigation?
- Hidden PII data fields in emails

U.S. AIR FORCE

Commanders/Directors, What Can You Do?

- Establish a Privacy Office
- Establish policies to notify MAJCOM/Wing Commanders of Privacy Act violations, complaints and breaches
- Establish policies necessary to implement and enforce the USAF Privacy Program
- Ensure all assigned USAF personnel are aware of and understand the requirements within AFI 33-332
- Ensure all privacy related issues or concerns are brought to the attention of servicing privacy manager or the USAF Privacy Officer
- Ensure all assigned personnel have completed required mandatory annual privacy training and specialized training when applicable

U.S. AIR FORCE

Commanders/Directors, What Can You Do?

- Submit an initial OPREP if it is determined the breach may have an impact on operations and or potential media attention (more than 5K also triggers OPREP)
- Appoint Investigating Official to conduct inquiry
- Determine if actual breach or policy violation has occurred
- Determine any criminal intent
- If warranted, ensure notifications are sent to affected personnel
- Ensure individual who caused breach completes refresher training
- If necessary, be punitive!!!

Commanders Have Options

U.S. AIR FORCE

Conclusion

- If you don't need PII for mission accomplishment DO NOT use it
- Encrypt emails containing PII
- Use approved methodologies if you cannot send encrypted emails (ARMDEC SAFE) (password protection)
- Practice safe handling procedures (regardless of media type)
- Notify your Privacy POC of any potential PII breach
- "We understand this may inconvenience our users; however, as an Operational Security imperative, protecting this data, your personal data, is the priority."; Honorable Matthew P. Donovan, USECAF

It's the LAW!!!

U.S. AIR FORCE

Questions

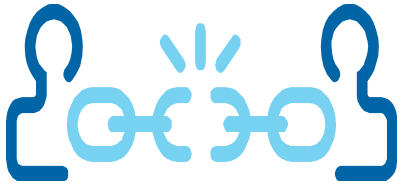
- POC: Mr. LaDonne L. White
- Email: ladonne.white.1@us.af.mil
- Comm Phone: 571-257-2515

Backup Slides

U.S. AIR FORCE

What is PII?

Per OMB A-130, the term PII refers to information that can be used to distinguish or trace and individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual



Types of PII

This is NOT an all-inclusive list.

Name	Race/Ethnicity	Driver's License	Home Phone
SSN	Education	Medical Information	Cell Phone
Rank/Grade	Financial	Religious Preference	Photo
Date of Birth	Marital Status	Emergency Contact	Military Records
Place of Birth	Gender	Dependent Information	Passport Information
Legal Status	Biometrics	Clearance Information	Work Phone/Email
DoD ID	Personal Email	Home Address	Work Address

Definition of a Breach

- A PII breach define by OMB M-17-12 is "the 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 personal identifiable information or
  - (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose"

HARM–EMBARASSMENT-INCONVIENCE

U.S. AIR FORCE

Breach Types

- Emails and attachments containing PII
- Mishandling of paper records/CDs containing PII
- Stolen/lost laptops or Government phones
- Improper access to shared drives
  - SharePoint!!!!!
- Inappropriate disposal of PII
- Sharing Information

U.S. AIR FORCE

SAF CIO Actions

- SAF CIO A6 met with Under Secretary to discuss PII breaches in effort to reduce/eliminate (9 Jan 18)
  - SAF CIO A6 tasked to develop plan of action to mitigate PII breaches in the AF
  - Safeguarding PII Commanders Call Topics (Jan/Feb 18)
  - Develop training for A1/FSS
- SAF CIO A6 sponsored Integrated Project Team (IPT) to tackle PII breaches in the AF (29 Jan – 1 Feb)
  - Plan to block all outgoing unencrypted emails containing PII

U.S. AIR FORCE

PII Block Rollout

- Under Secretary's remarks: “We understand this may inconvenience our users; however, as an Operational Security imperative, protecting this data, your personal data, is the priority. “
- By direction of the Under Secretary of the Air Force, an order was initiated to block email traffic containing unprotected PII immediately. (12 Feb 17)
- Three tools to provide enterprise coverage to the vast majority of AF users.
  - a – MacAfee Email Gateways (MEG) (9 Feb 18)
  - b – Digital Signature Enforcement Tool (DSET) (28 Feb 18)
  - c – Cloud Hosted Enterprise Services (CHES) (18 Mar 18)
- AF.MIL article released Feb 2018 http://www.af.mil/News/Article-Display/Article/1436362/air-force-to-institut e-new-method-to-protect-pii/ to highlight the effort.