U.S. AIR FORCE
OFFICE OF THE CHIEF INFORMATION SECURITY OFFICER (CISO)

To assure the effectiveness of Air Force's core missions by increasing the cybersecurity and resiliency of systems and information.

DATA PRIVACY DAY

OMB M 17-12: Preparing for and Responding to a Breach of Personally Identifiable Information (PII)

Prevent

Ensure that personnel are informed about how to properly respond to a breach or incident. Training and awareness content should include:

- How and why to safely identify, handle, store, transmit, and dispose of PII
- Any consequences of noncompliance
- Reporting requirements in the event of an incident
- Key definitions of PII, breach, and incident

Additionally, every base should have a robust **breach response plan** in place so that remediation activities are both quick and effective.

QUICKTIP: Schedule bi-annual or more frequent breach response plan updates to make necessary adjustments based on evolving threats or DoD "lessons learned."

Report

It is critical that every confirmed PII breach or incident is immediately reported to the following entities in a timely manner:

- US-CERT (within 1 hour of breach)
- Law Enforcement
- The Inspector General
- General Counsel
- Congress (committees pursuant to FISMA)

*What is a breach?**

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 personally identifiable information or
(2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose.

Assess

In the event of a breach or incident, each base's privacy officer should determine the risk of harm to potentially affected personnel, considering:

- Type of breach, taking into account the intent and recipient(s) of the breach
- Nature and sensitivity of PII
- Likelihood of access by an unauthorized individual

Respond

Upon assessing risk of harm to individuals affected by a breach, the department's privacy officer should, on a case-by-case basis:

- Apply timely countermeasures such as requiring users to change compromised passwords
- Provide guidance on how to reduce identity theft and how to manage potentially affected accounts
- Provide ID protection services to certain affected individuals. BPAs are available with trusted providers.

It is not always required to notify affected individuals, depending on the nature of the breach. The Air Force should balance urgency in notifying individuals with knowing all facts about the breach.

***For more information, please refer to OMB M-17-12**