INFORMATION PAPER

SFAE-HR June 2009

SUBJECT: Personally Identifiable Information (PII)

1. Purpose. To provide information on the US Army Acquisition Support Center (USAASC) policy and procedures safeguarding PII for the Army Acquisition Corps' (AAC).

2. Facts.

   a. USAASC prepares a memorandum to PEOs/DRPMs, outlining the rules and consequences policy for safeguarding PII.

   b. Each PEO/DRPMs is responsible for ensuring all Soldiers and civilians know what PII is and are aware of the consequences for release of the PII.

   c. PII is any information that can be used to distinguish or trace an individual's identity, such as their name, social number, biometric records either alone or when combined with other personal or identifying information which is linked or linkable to a specific individual such as, date of birth, mother's maiden name, etc.

   d. Each PEO/DRPM must report all cases of actual or suspected breach of PII. A complete review of the facts and circumstances related to the breach will be investigated and if necessary disciplinary action will be taken.

   e. Ensure reporting and notification occurs IAW the following procedures. Report all incidents involving actual or suspected breach/compromise of PII to the United States Computer Emergency Readiness Team (US-CERT) within one hour of discovery. Reports must be submitted at Http://www.us-cert-gov. An email will be sent to PIIReporting@us.army.mil which notifies Army leadership that an initial report has been submitted to US-CERT. The email should provide a brief synopsis, POC and contact information for the incident.

   f. The organization possessing or responsible for safeguarding the PII at the time of the incident must notify the affected individuals as soon as possible, but NLT 10 days after the breach/compromise is discovered.

Helene Kelsey/703-805-1012