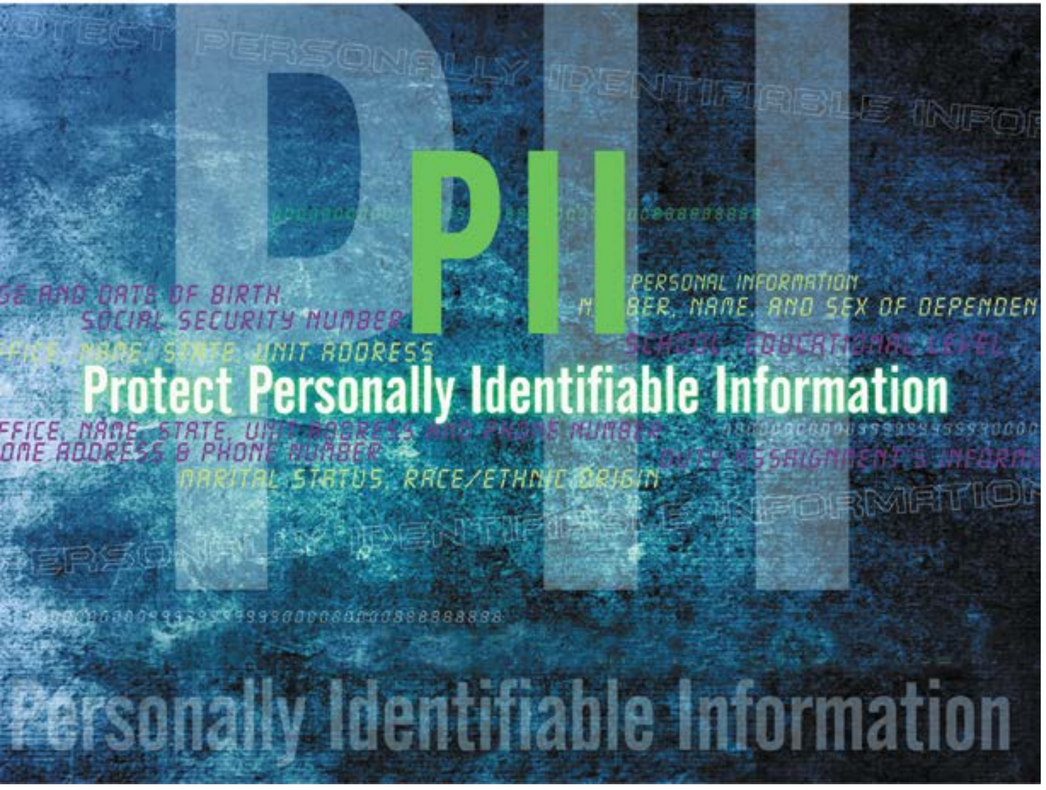
# Think before sending: Protecting PII




Art by Naoko Shimoji

PII is unique information about an individual not releasable to the public without the written consent of the individual. Examples includes Social Security numbers, dates of birth, marital status, race or financial information.

**By Maj. Brooke Brander**
Air Force Space Command Public Affairs
**Wayne Amann**
Air Force Intelligence Surveillance and Reconnaissance Agency Public Affairs
**Leslie Finstein**
502nd Air Base Wing Public Affairs

Network security is more than just a buzzword. It is an important tool used to secure not just information related to national security but also personal security. The Air Force, Army and the entire Department of Defense take information assurance and the protection of personal information seriously.

As of October 2013, individuals who inappropriately store and transmit personally identifiable information over the Air Force network will have their accounts locked in response to the violation.

"We are taking several steps to improve notification and reporting of PII incidents," said Gen. William L. Shelton, Air Force Space Command commander. "My intent is to increase awareness within the Air Force as part of my responsibility to ensure the security and defense of the AFNET and its users. PII violations create both personal and operational risks for all of us."

Air Force Space Command is the major command responsible for Air Force space and cyber operations. Cyber operations are organized under 24th Air Force, headquartered at Joint Base San Antonio-Lackland.

PII is any information about an individual that can be used directly, or in connection with other data, to identify, contact or locate that person and can include such information as: full name, address, Social Security number, medical, educational, financial, legal and employment records.

This information can come in any form such as hard copy or electronic records stored within data bases or accessible from applications on computers, laptops and electronic devices (government or private) such as Blackberries, smartphones', etc.

The 68th Network Warfare Squadron and 352nd Network Warfare Squadron on JBSA-Lackland, as the Cyberspace Defense Analysis Weapon System, actively monitors the AFNET for PII breaches and violations. When a PII breach is identified, it is reported to the 624th Operations Center, also on JBSA-Lackland, and the formal reporting process is initiated.

The 624th OC, as the Cyber Command and Control Mission System Weapon System, then reports the AFNET PII breach to the 24th Air Force commander, which will result in locking the violator's AFNET account and notification to the individual's wing commander.

"Beginning Oct. 24, [2013] we began locking out the AFNET account of individuals who were found to be inappropriately transmitting PII data via the AFNET," explained Maj. Gen. J. Kevin McLaughlin, 24th Air Force and Air Force Cyber commander. "A violator's account will only be unlocked once the first O-6 in their chain of command certifies that the individual has accomplished all necessary actions, to include remedial training."

These new actions are in addition to, and do not circumvent or replace, the normal Privacy Act notification process which is already in place throughout the Air Force. Air Force Instruction 33-332 governs the PII breach reporting process as well as the consequences for PII violations.

A PII breach is defined as a 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 an other than authorized purpose, have access or potential access to PII, whether physical or electronic.

For those on the AFNET, JBSA follows the Air Force protocols for PII breaches, requiring individuals who lose network access as the result of a breach to receive authorization from a colonel in their chain of command to reactivate their account and to contact their local information assurance office and customer or client support technician, said Karen Frey, JBSA Freedom of Information Act and Privacy Act officer.

For JBSA personnel operating on the Army network, an individual's unit leadership determines whether their user account is disabled based on the initial assessment of the U.S. Army Signal Network Enterprise Center, said Jesus RosaVelez, NEC director for JBSA.

Further punitive actions against individuals responsible for a breach, RosaVelez continued, are based on the finalized report and seriousness of the incident.

The majority of PII breaches are directly the result of human error either by the individual directly or by second or third parties, said RosaVelez.

Since his arrival at JBSA in May 2012, RosaVelez knows of two reported official incidents on the Army network here.

There was a unit that failed to set proper permissions on folder access on a storage drive which could have potentially compromised PII data saved in those folders.

An individual on the Army network here also once accidentally forwarded a series of unencrypted emails containing social security numbers to unit distribution list email address.

RosaVelez stressed that just because these are the only two he knows of that does not mean other incidents have not occurred. Other units may not have reported incidents to the NEC which is in violation of PII policy.

Units must report all suspected breaches.

"The loss of PII can erode confidence in the ability to protect information, impact business practices and can lead to major legal action," RosaVelez said.

Frey recommends personnel kicked off the network for PII violations complete the online training course, the 'CyberAwareness Challenge.' It is an annual requirement for all federal, Department of Defense and intelligence community personnel.

According to the Information Assurance Education, Training and Awareness online training catalog, the 'CyberAwareness Challenge' course is a serious game that simulates key decision points that employees make every day in the course of their duties that could either protect or compromise PII.

The training can be found online at http://iase.disa.mil/eta/online-catalog.html#iaatraining

When working with PII, personnel are urged to follow these common sense precautions:

- Do not transmit PII to or from personal or commercial email accounts unless a written consent has been submitted by each individual requesting their personal information be sent to their personal or commercial email account.
- Do not mail or courier sensitive PII on electronic removable media unless the data is encrypted.
- Do not leave PII in unsecured vehicles, unattended workspaces, unsecure file drawers or in checked baggage.
- Do not store or use PII on personal media.
- Reduce Social Security number usage within the Department of Defense communiqués and limit the use of the SSN(s) in any form (including the last four digits) in addition to substituting the user of identification numbers or any unique identifier whenever possible.
- Never include SSN(s) in a personnel roster or other documents when not necessary. SSN(s) must never be posted on public facing websites.
- Use only officially issued forms by applicable service; especially those that collect PII should include the Privacy Act Statement.

"One breach is too many," said Maj. Gen. John Shanahan, Air Force Intelligence, Surveillance and Reconnaissance Agency commander. "A PII breach is neither acceptable nor excusable. It comes down to adhering to well-established guidelines, rules and procedures."

If you see a PII breach, immediately notify your chain of command or organization privacy act manager/monitor.

Commanders, managers, supervisors should ensure that everyone within their units are familiar with "personally identifiable information (pii) incident reporting and notification procedures."

"The report of PII incidents involving actual or suspected breaches/compromises should be reported immediately; preferably within one hour of discovery," said RosaVelez.

"Accountability is the word of the day," Shanahan said. "I expect everyone in the enterprise to be accountable for protecting PII. We need maximum emphasis on this because the downsides of a breach are obvious."

Graphic by Chief Master Sgt. John Zincone

Multiple methods to encrypt sensitive information exist and are available for use. AFNet users can encrypt information leaving the AFNet by using the AF Research Lab's encryption wizard, the encryption capabilities of Microsoft Office or by sending the documents by mail.

## U.S AND DOD GUIDANCE

»U.S.C. 552a, The Privacy Act of 1974
»AR 340-21, The Army Privacy Program
»AR 380-5, Department of the Army Information Security Program
»AFI 33-332, Air Force Privacy and Civil Liberties Program
»NETCOM Regulation 25-56 2
»NETCOM Regulation 190-1, Serious Incident Reporting
»DOD 5400.11-R, Department of Defense Privacy Program
Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems (http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf)
»DD Form 2930, Privacy Impact Assessment (PIA)
»NETCOM Form 190-1-1, Serious Incident Report
»U.S. Army Records Management and Declassification Agency (RMDA) Privacy Office website (https://www.rmda.army.mil/organization/pa.shtml)

## RELATED LINKS

Users at Joint Base San Antonio have multiple tools at their disposal to protect PII if encrypting e-mail is not feasible and electronic transmission of sensitive PII is operationally required. Users can leverage approved Department of Defense safe file transfer systems.

Safe Access File Exchange - https://safe.amrdec.army.mil/safe/