From IA Messaging **Date** Friday, December 09, 2011 1:21:19 PM
To All_IA
Cc
Subject Handling Sensitive Information Within Indian Affairs

The Privacy Act of 1974, as amended, requires that sensitive information, which is defined to include data that could be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual, be properly protected from exposure to unauthorized individuals. Personally Identifiable Information (PII) is the widely accepted abbreviation but the phrase has four common variants based on personal, personally, identifiable and identifying. The Department of the Interior (DOI) and Indian Affairs (IA) policy (65 IAM 4) specifically require that PII stored on mobile media be encrypted using a FIPS-140-2 compliant device. Failure to comply with DOI and IA policy may result in significant disciplinary action.

Should an employee or contractor suspect or have knowledge that PII has potentially been exposed to unauthorized individuals or if a mobile electronic device has been lost, then the knowledgeable individuals are required to report the event to the Bureau Privacy Officer within one hour. The Indian Affairs Privacy Act Officer is Ms. Willie Chism. She may be contacted at 703-735-4163 or 703-539-9486 or by e-mail at Willie.Chism@bia.gov

Each year employees and contractors receive information security and privacy training to emphasize the importance of protecting sensitive information (including PII) and the potential consequences for violating policies regarding the protection of sensitive information. Additional information concerning PII and security requirements is available at https://sp.ia.doi.net/sites/ASIA/ocio/disp/si ."

Assistant Director for Information Resources