From IA Messaging **Date** Mon Apr 09 2012 17:04:39 GMT-0400 (Eastern Daylight Time)

To All_IA; All IE

Cc

Subject Consequences for Unauthorized Disclosure of Sensitive Information

All Employee Message

To follow up on the December 9, 2011 "All Employee Message" entitled Handling Sensitive Information within Indian Affairs, this message provides individuals with information about the remedial actions that will be taken when it is discovered that employees or contractors use email to disclose or potentially disclose sensitive information. The unauthorized disclosure of sensitive information may occur when information, including an individual's Personally Identifiable Information (PII), is emailed to an unsecured destination outside of the bia.gov domain.

The Privacy Act of 1974 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. Each year employees and contractors receive information security and privacy training to emphasize the importance of protecting sensitive information (including PII), and to understand the potential consequences for violating policies regarding the protection of sensitive information. In addition, each year employees are required to take the Rules of Behavior Certification online through DOI Learn and acknowledge that they understand their responsibilities to protect sensitive information.

To protect sensitive data, the Indian Affairs Computer Security Incident Response Team (CSIRT) along with the Indian Affairs Messaging Team and the Department of the Interior Advanced Security Operations Center (ASOC) monitor each email message and email attachment using sophisticated security software for the purpose of detecting the unauthorized use of sensitive data. When it is discovered that sensitive data, including PII, is put at risk, individuals must be held accountable for their actions.

To encourage a higher level of compliance, the Indian Affairs Office of Information Security and Privacy (OISP) is strengthening security protocols. These new security protocols include:

- Immediate disabling of access to computer resources
- Requiring supervisor intervention to reinstate computer access
- Recommending other appropriate remedial actions, including the completion of required training, administrative actions, or termination.

Existing procedures related to the release of PII and other sensitive information is included in the Departmental Manual (DM) Part 370: Departmental Personnel Program Chapter 752.1: Discipline and Adverse Actions. This chapter identifies penalties for first, second, and third offenses and includes situations where information is not compromised, and where release is unintentional. Supervisors and employees are encouraged to review these sanctions to understand the potential outcome of inappropriate system use and unauthorized information disclosure.

If you have any questions you may contact the Indian Affairs Privacy Act Officer, Ms. Willie Chism at 703-735-4163, 703-539-9486 (mobile) or by e-mail at Willie.Chism@bia.gov