

February 4, 2010

TO: Bureau Chief Financial Officers, Principal Human Resources Managers, Chief Information Officers and Security Directors

1. Why we're holding this meeting:

To discuss our collective responsibility for protecting Personally Identifiable Information (PII).

Breaches of PII throughout our increasingly wired society have increased dramatically over the past few years and have resulted in the loss of millions of records. Breaches of PII can be detrimental to both individuals and organizations. Individual harms from breaches may include identity theft, embarrassment or blackmail. Organizational harms may include a loss of public or employee trust, legal liability or high costs to handle the breach.

You in the course of your daily activities, have access to employee PII, including SSNs, home addresses, medical information, benefit, salary and contact information. It is our inherent job responsibility to protect PII by following Department and government-wide policies and put office procedures in place where necessary (e.g., shredders, requirements about encryption policies).

2. What is PII

PII is information which can be used to distinguish or trace an individual's identity, such as their name, SSN, fingerprint records, date and place of birth, mother's maiden name, etc.

PII can be in the form of electronic documents, physical documents and/or verbal conversations and voice recordings.

3. When to protect PII

Protect PII both electronic and physical forms at all times.

Anytime PII is transmitted electronically it **MUST BE ENCRYPTED** following Departmental encryption policy – encrypt it even if the email is sent to your suite mate that works off the same IT environment.

4. How to protect PII

Encrypt all PII when electronically transmitted, lock up or shred PII when in the physical form, and be discrete in your conversations when discussing PII – a “need to know” practice is best.

Train your staff on how to protect and specifically how to encrypt a document containing PII.

Monitor employee practices when handling PII and address employee behavior when rules are knowingly and intentionally not followed.

Make sure your staff knows and follows established procedures and policies.

5. When to report a PII loss

The Department IT Security Program Policy, released January of 2009, requires that each Bureau have a formal, documented, incident response policy and capability that addresses roles, responsibilities, coordination among organizational entities, and compliance. For incidents which involve the suspected or confirmed breach or loss of PII, reporting shall be immediate to the Operating Unit (OU) Incident Response Team (OU-IRT). The OU-IRT will report the incident to the Commerce Incident Response Team (CIRT), and, within one hour, to the United States Computer Emergency Readiness Team (US-CERT).

There is a standing ID Theft Task Force at the Department that reviews all reported PII-related incidents and determines whether notification to employees is required.

6. Since Early December 2009

We have experienced three incidents where either human or system errors resulted in a potential for loss of PII. Two of these incidents occurred last week. These incidents involved a few hundred employees and we have no reason to believe any personal information was inappropriately used by anyone.

In addition to the incidents themselves, our procedure for notification within the Department was not always correctly followed. Department management was not made aware of follow up communication to affected employees until after communication had been sent to affected employees. Such departure from protocol can make a serious mistake even worse.

7. What is the Department doing to improve the protection of PII

The Secretary has ordered a task force to be formed to conduct a 360-degree review of the existing PII policy, notification procedures and ID theft task force processes, and that its work will be completed by March 1, 2010. This work is to include revisions and the strengthening of the policy and procedures.

The Secretary is also sending a broadcast e-mail about protecting PII to all Commerce employees.

The Deputy Secretary held an emergency executive management team (EMT) meeting yesterday to discuss this issue and the importance of properly handling PII.