DEC 3 1 2009

UNITED STATES DEPARTMENT OF COMMERCE
Chief Financial Officer and
Assistant Secretary for Administration
Washington, D.C. 20230

Dear Commerce Employee:

The Purpose of this letter is to notify you of a breach of protocol involving your Personally Identifiable Information (PII), including your social security number (SSN) and name.

On December 4, 2009, a Department of Commerce employee inadvertently transmitted over the Internet a file containing the PII of Commerce employees to other Department employees. Although the Department employees were authorized to send and receive the PII, the transmission of the PII over the Internet in unencrypted form may have compromised your name and SSN. As soon as the Department employee recognized the error, the supervisor and the Department's IT Security staff were notified. The IT Security Staff took the appropriate measures to investigate and mitigate the breach.

The Department is taking necessary steps to protect and inform those affected by this possible compromise. While we have no indication that your PII was, in fact, compromised by this breach, the Department takes all potential compromises very seriously. It is, therefore, procuring the services of a third-party vendor who will monitor the exposed data to determine if identity theft is occurring as a result of this breach. Should the vendor make that determination, the Department will notify you immediately and detail additional steps that need to be taken.

We also encourage you to contact one of three nationwide, consumer reporting companies and place an "initial fraud alert" on your credit file. This alert can help stop someone form opening new credit accounts in your name. You can make a free, initial fraud alert request, as well as obtain additional services, by contacting:

Equifax: www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241;

Experian: 1-888-EXPERIAN (397-3742); https://www.experian.com/fraud/center.html; P.O. Box 2002, Allen, TX 75013; or

TransUnion: 1-800-680-7289; http://www.transunion.com/corporate/personal/fraudIdentityTheft/fraudPrevention/fraudAlert.page; Fraud Victim Assistance Division, P.O. Box, Fullerton, CA 92834-6790.

More information on fraud reports and what to watch for to ensure your information is not being misused is available at the Federal Trade Commission's website at http://www.ftc.gov/bcpedu/pubs/consumer/alerts/alt150.pdf.

Please contact idtheft@doc.gov if you have any follow-up questions that we may be able to answer and particularly if you are notified by the credit bureaus of any suspicious credit file activity, especially any unauthorized attempts to open new accounts in your name.

Senior Department leadership was briefed on this incident and is committed to taking every precaution necessary to limit the exposure of your SSN. This unfortunate incident was caused by an oversight due to SSNs being hidden in a spreadsheet.

The Department of Commerce will take additional steps if monitoring by our third-party vendor, or by employees, suggests that your PII has been exposed by this protocol breach.

If you have questions, please contact your servicing personnel office.

Sincerely,

for Deborah A. Jefferson
Deputy Chief Human Capital Officer and
Director for Human Resources Management