U.S. Department of Justice

Office of the Deputy Attorney General

Washington, D.C. 20530

July 10, 2006

MEMORANDUM FOR HEADS OF DEPARTMENT COMPONENTS

FROM: Paul J. McNulty PJM
Deputy Attorney General

SUBJECT: Review of Policies and Processes to Ensure Adequate Safeguards to Protect Personally Identifiable Information

The Office of Management and Budget (OMB) Memorandum on Safeguarding Personally Identifiable Information, dated May 22, 2006, (M-06-15), requires each agency's senior official for privacy to conduct a review of agency policies and processes to ensure the agency "has adequate safeguards to prevent the intentional or negligent misuse of, or unauthorized access to, personally identifiable information." OMB further directs that "[t]his review shall address all administrative, technical, and physical means used by your agency to control such information, including but not limited to procedures and restrictions on the use or removal of personally identifiable information beyond agency premises or control." In order for the Department Chief Privacy and Civil Liberties Officer (CPCLO) to conduct this review for the Department, I am asking that each of you conduct such a review with respect to your component and report the results of your review to the CPCLO. Include in the report existing component procedures and policies on the use or removal of personally identifiable information beyond agency premises or control. The results of the Department review must be included in the Department's upcoming Federal Information Security Management Act (FISMA) compliance report, which is due to OMB in early October. Therefore, your report must be submitted to the CPCLO by August 25, 2006.

In a separate memorandum, I am reminding all employees of the need to immediately report the loss or compromise of any personally identifiable information, including information in paper and electronic form, to their supervisor. I ask that you review your component's procedures for reporting such information, and designate a component official who would be responsible for receiving such information and promptly reporting significant losses to the CPCLO. Please provide the CPCLO with contact information for the individual you have designated by August 31, 2006. The CPCLO will provide further guidance to this individual on which losses are considered "significant" and should be reported to the CPCLO.

U.S. Department of Justice

Office of the Deputy Attorney General

Washington, D.C. 20530

July 10, 2006

MEMORANDUM FOR ALL DEPARTMENT EMPLOYEES

FROM: Paul J. McNulty PJM
Deputy Attorney General

Jane C. Horvath
Chief Privacy and Civil Liberties Officer

SUBJECT: Privacy and Safeguarding of Personally Identifiable Information

In response to recent events, this memorandum serves to remind all Department employees of their responsibility to safeguard and protect personally identifiable information about individuals from improper access or disclosure. As employees of the Department, many of you have access to and work with sensitive information about individuals in the performance of your official duties. It is important that you are generally familiar with your responsibilities that come with handling that data as improper disclosures can be harmful to the individual in question as well as to the Department's mission.

- As a general matter, Departmental regulations state employees should be mindful of their responsibility to protect and conserve Government property, which includes Government records. See 28 C.F.R. § 45.4(c); 5 C.F.R. § 2635.704.

- You should not disclose personally identifiable information about an individual to persons outside the Department other than for an authorized official business purpose.

- Disclosure of personally identifiable information within the Department is subject to a need to know standard. In other words, you may reveal information about an individual only to others within the Department who have a need for the information in the performance of their official duties.

- Additionally, some personally identifiable information is covered by the requirements of the Privacy Act of 1974, 5 U.S.C. § 552a. The disclosure of Privacy Act records within the Department are covered by the same need to know standard described above. For disclosures of Privacy Act records outside the Department, a statutory exception in the Privacy Act or a published routine use must authorize such disclosure or the disclosure must be otherwise provided for by law. There are criminal penalties for willful unauthorized disclosures under the Privacy Act.

- To prevent unauthorized disclosures, employees should follow all applicable Departmental rules for safeguarding personally identifying information.

- Report any loss or compromise of personally identifying data to your supervisor immediately.

Please discuss with your supervisor any further questions regarding how to handle personally identifiable information or whether information is considered personally identifiable information.