EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

May 22, 2006

M-06-15

MEMORANDUM FOR THE HEADS OF DEPARTMENTS AND AGENCIES

FROM: Clay Johnson III
Acting Director

SUBJECT: Safeguarding Personally Identifiable Information

As you know, the loss of personally identifiable information can result in substantial harm, embarrassment, and inconvenience to individuals and may lead to identity theft or other fraudulent use of the information. Because Federal agencies maintain significant amounts of information concerning individuals, we have a special duty to protect that information from loss and misuse.

This memorandum reemphasizes your many responsibilities under law and policy to appropriately safeguard sensitive personally identifiable information and train your employees on their responsibilities in this area. In particular, the Privacy Act requires each agency to establish:

> "rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or maintaining any record, and instruct each such person with respect to such rules and the requirements of [the Privacy Act], including any other rules and procedures adopted pursuant to this [Act] and the penalties for noncompliance", and
>
> "appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained." (5 U.S.C. § 552a(e)(9)-(10))

Early last year, I directed each agency to designate a Senior Agency Official for Privacy at the Assistant Secretary-level or equivalent (Memorandum M-05-08), and all agencies have done so, designating a senior official with overall responsibility and accountability for ensuring the agency's implementation of information privacy protections. (See http://www.whitehouse.gov/omb/egov/documents/SAOPcontactlistfinal.pdf)

Please have your agency's Senior Official for Privacy conduct a review of your policies and processes, and take corrective action as appropriate to ensure your agency has adequate safeguards to prevent the intentional or negligent misuse of, or unauthorized access to, personally identifiable information. This 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. This review shall be completed in time for you to include the results in your upcoming reports due this fall on compliance with the Federal Information Security Management Act (FISMA). Include any weaknesses you identify in your security plans of action and milestones already required by FISMA. In addition, please ensure your agency employees are reminded within the next 30 days of their specific responsibilities for safeguarding personally identifiable information, the rules for acquiring and using such information as well as the penalties for violating these rules.

Finally, I want to remind you of your responsibilities under FISMA and related policy to promptly and completely report security incidents to proper authorities, including Inspectors General and other law enforcement authorities. In certain circumstances, this reporting also includes the Department of Homeland Security (DHS). Last year, the Office of Management and Budget provided to your Chief Information Officer the specific requirements including timelines for reporting to DHS. Copies of these mandatory requirements are available from the DHS National Cyber Security Division.